Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
10web					
photo_gallery					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-21	4.3	The Photo Gallery by 10Web WordPress plugin before 1.5.68 is vulnerable to Reflected Cross-Site Scripting (XSS) issues via the bwg_album_breadcrumb_0 and shortcode_id GET parameters passed to the bwg_frontend_data AJAX action **CVE ID : CVE-2021-25041**	https://plugins.trac.wordpress.org/changeset/2467205	A-10W-PHOT-201221/1
accops					
hyworks_dvm_tools					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	A Buffer Overflow vulnerability exists in Accops HyWorks DVM Tools prior to v3.3.1.105. The IOCTL Handler 0x22001B allows local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42681**	N/A	A-ACC-HYWO-201221/2
Integer Overflow or Wraparound	07-Dec-21	7.2	An Integer Overflow vulnerability exists in Accops HyWorks DVM Tools prior to v3.3.1.105 .The IOCTL Handler 0x22001B allows	N/A	A-ACC-HYWO-201221/3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42682**		
Integer Overflow or Wraparound	07-Dec-21	7.2	An Integer Overflow vulnerability exists in Accops HyWorks DVM Tools prior to v3.3.1.105 . The IOCTL Handler 0x22005B in the Accops HyWorks DVM Tools prior to v3.3.1.105 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42685**	N/A	A-ACC-HYWO-201221/4
hyworks_windows_client					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	A Buffer Overflow vulnerability exists in Accops HyWorks Windows Client prior to v 3.2.8.200. The IOCTL Handler 0x22001B allows local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42683**	N/A	A-ACC-HYWO-201221/5
Integer Overflow or Wraparound	07-Dec-21	7.2	An Integer Overflow exists in Accops HyWorks Windows Client prior to v 3.2.8.200. The IOCTL Handler	N/A	A-ACC-HYWO-201221/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0x22001B in the Accops HyWorks Windows Client prior to v 3.2.8.200 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	A Buffer Overflow vulnerability exists in Accops HyWorks Windows Client prior to v 3.2.8.200. The IOCTL Handler 0x22005B allows local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42687**	N/A	A-ACC-HYWO-201221/7
Integer Overflow or Wraparound	07-Dec-21	7.2	An Integer Overflow vulnerability exists in Accops HyWorks Windows Client prior to v 3.2.8.200. The IOCTL Handler 0x22005B in the Accops HyWorks Windows Client prior to v 3.2.8.200 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42688**	N/A	A-ACC-HYWO-201221/8
Admidio					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
admidio					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-21	4.3	Admidio is a free open source user management system for websites of organizations and groups. A cross-site scripting vulnerability is present in Admidio prior to version 4.0.12. The Reflected XSS vulnerability occurs because redirect.php does not properly validate the value of the url parameter. Through this vulnerability, an attacker is capable to execute malicious scripts. This issue is patched in version 4.0.12. **CVE ID : CVE-2021-43810**	https://github.com/Admidio/admidio/commit/fcb0609abc1d2f65bc1377866bd678e5d891404b, https://github.com/Admidio/admidio/commit/c043267d362f7813543cc2785119bf3e3e54fe21, https://github.com/Admidio/admidio/security/advisories/GHSA-3qgf-qgc3-42hh	A-ADM-ADMI-201221/9
Adobe					
bridge					
Out-of-bounds Read	07-Dec-21	4.3	Adobe Bridge versions 11.1.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious RGB file.	https://helpx.adobe.com/security/products/bridge/apsb21-94.html	A-ADO-BRID-201221/10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-44185		
Out-of-bounds Read	07-Dec-21	4.3	Adobe Bridge versions 11.1.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious SGI file. **CVE ID : CVE-2021-44186**	https://helpx.adobe.com/security/products/bridge/apsb21-94.html	A-ADO-BRID-201221/11
Out-of-bounds Read	07-Dec-21	4.3	Adobe Bridge versions 11.1.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious SGI file. **CVE ID : CVE-2021-44187**	https://helpx.adobe.com/security/products/bridge/apsb21-94.html	A-ADO-BRID-201221/12
ajaxpro.2_project					
ajaxpro.2					
Deserialization of Untrusted Data	03-Dec-21	7.5	All versions of package ajaxpro.2 are vulnerable to Deserialization of Untrusted Data due to the possibility of deserialization of arbitrary .NET classes, which can be abused to gain remote code	https://github.com/michaelschwarz/Ajax.NET-Professional/commit/b0e63be5f0bb20dfce507cb8	A-AJA-AJAX-201221/13

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2021-23758**	a1a9568f6e73de57, https://snyk.io/vuln/SNYK-DOTNET-AJAXPRO2-1925971	
Allegro					
allegro					
N/A	08-Dec-21	6.2	An issue was discovered in Allegro Windows (formerly Popsy Windows) before 3.3.4156.1. A standard user can escalate privileges to SYSTEM if the FTP module is installed, because of DLL hijacking. **CVE ID : CVE-2021-42110**	https://excellium-services.com/cert-xlm-advisory/CVE-2021-42110, http://www.popsy.com/Documents/Setups/Setup.Allegro.3.3.4154.2.exe	A-ALL-ALLE-201221/14
Insufficiently Protected Credentials	08-Dec-21	5.5	Allegro WIndows 3.3.4152.0, embeds software administrator database credentials into its binary files, which allows users to access and modify data using the same credentials. **CVE ID : CVE-2021-43978**	https://www.allegro.be/, https://excellium-services.com/cert-xlm-advisory/CVE-2021-43978	A-ALL-ALLE-201221/15
Amazon					
sockeye					
Improper Control of Generation of Code ('Code	08-Dec-21	6.8	Sockeye is an open-source sequence-to-sequence framework for Neural Machine Translation built on PyTorch. Sockeye uses YAML	https://github.com/awslabs/sockeye/security/advisories/GHSA	A-AMA-SOCK-201221/16

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			to store model and data configurations on disk. Versions below 2.3.24 use unsafe YAML loading, which can be made to execute arbitrary code embedded in config files. An attacker can add malicious code to the config file of a trained model and attempt to convince users to download and run it. If users run the model, the embedded code will run locally. The issue is fixed in version 2.3.24. **CVE ID : CVE-2021-43811**	-ggmr-44cv-24pm, https://github.com/awslabs/sockeye/pull/964	
workspaces					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	Amazon WorkSpaces agent is affected by Buffer Overflow. IOCTL Handler 0x22001B in the Amazon WorkSpaces agent below v1.0.1.1537 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-43637**	N/A	A-AMA-WORK-201221/17
Integer Overflow or Wraparound	07-Dec-21	7.2	Amazon Amazon WorkSpaces agent is affected by Integer Overflow. IOCTL Handler 0x22001B in the Amazon WorkSpaces agent below v1.0.1.1537 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory	N/A	A-AMA-WORK-201221/18

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-43638**		
AMD					
amd_uprof					
Improper Privilege Management	01-Dec-21	9	The AMDPowerProfiler.sys driver of AMD ?Prof tool may allow lower privileged users to access MSRs in kernel which may lead to privilege escalation and ring-0 code execution by the lower privileged user. **CVE ID : CVE-2021-26334**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1016	A-AMD-AMD_-201221/19
amzetta					
zportal_dvm_tools					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	Amzetta zPortal DVM Tools is affected by Buffer Overflow. IOCTL Handler 0x22001B in the Amzetta zPortal DVM Tools <= v3.3.148.148 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-43002**	N/A	A-AMZ-ZPOR-201221/20
Integer Overflow or Wraparound	07-Dec-21	7.2	AmZetta Amzetta zPortal DVM Tools is affected by Integer Overflow. IOCTL Handler 0x22001B in the Amzetta zPortal DVM Tools <= v3.3.148.148 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory	N/A	A-AMZ-ZPOR-201221/21

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-43006**		
zportal_windows_zclient					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	Amzetta zPortal Windows zClient is affected by Buffer Overflow. IOCTL Handler 0x22001B in the Amzetta zPortal Windows zClient <= v3.2.8180.148 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-43000**	N/A	A-AMZ-ZPOR-201221/22
Integer Overflow or Wraparound	07-Dec-21	7.2	Amzetta zPortal Windows zClient is affected by Integer Overflow. IOCTL Handler 0x22001B in the Amzetta zPortal Windows zClient <= v3.2.8180.148 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-43003**	N/A	A-AMZ-ZPOR-201221/23
Apache					
airavata_django_portal					
Improper Encoding or Escaping of Output	09-Dec-21	5	Apache Airavata Django Portal allows CRLF log injection because of lack of escaping log statements. In particular, some HTTP	https://lists.apache.org/thread/q64h16ofdxk29soz3jj561nysnzc	A-APA-AIRA-201221/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request parameters are logged without first being escaped. Versions affected: master branch before commit 3c5d8c7 [1] of airavata-django-portal [1] https://github.com/apache/airavata-django-portal/commit/3c5d8c72bfc3eb0af8693a655a5d60f9273f8170 **CVE ID : CVE-2021-43410**	rl31	
log4j					
Deserialization of Untrusted Data	10-Dec-21	9.3	Apache Log4j2 <=2.14.1 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. In previous releases (>2.10) this behavior can be mitigated by setting system property "log4j2.formatMsgNoLookups" to “true” or it can be mitigated in prior releases (<2.10) by removing the JndiLookup class from the classpath (example: zip -q -d log4j-core-*.jar org/apache/logging/log4j/co	https://logging.apache.org/log4j/2.x/security.html, https://security.netapp.com/advisory/ntap-20211210-0007/, https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0032, https://www.oracle.com/security-alerts/alert-cve-2021-44228.html	A-APA-LOG4-201221/25

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			re/lookup/JndiLookup.class). **CVE ID : CVE-2021-44228**		
Apereo					
central_authentication_service					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-21	4.3	Apereo CAS through 6.4.1 allows XSS via POST requests sent to the REST API endpoints. **CVE ID : CVE-2021-42567**	https://apereo.github.io/2021/10/18/restvuln/	A-APE-CENT-201221/26
Atlassian					
jira_software_data_center					
Improper Authentication	08-Dec-21	5	Affected versions of Atlassian Jira Server and Data Center allow a user who has had their Jira Service Management access revoked to export audit logs of another user's Jira Service Management project via a Broken Authentication vulnerability in the /plugins/servlet/audit/resource endpoint. The affected versions of Jira Server and Data Center are before version 8.19.1. **CVE ID : CVE-2021-41309**	https://jira.atlassian.com/browse/JRASERVER-72803	A-ATL-JIRA-201221/27
Improper Authentication	08-Dec-21	5	Affected versions of Atlassian Jira Server and Data Center allow attackers with access to an administrator account that has had its access revoked to modify projects' Users & Roles settings, via a Broken Authentication vulnerability	https://jira.atlassian.com/browse/JRASERVER-72802	A-ATL-JIRA-201221/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the /plugins/servlet/project-config/PROJECT/roles endpoint. The affected versions are before version 8.19.1. **CVE ID : CVE-2021-41311**		
attendance_management_system_project					
attendance_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Dec-21	7.5	attendance management system 1.0 is affected by a SQL injection vulnerability in admin/incFunctions.php through the makeSafe function. **CVE ID : CVE-2021-44280**	N/A	A-ATT-ATTE-201221/29
auth0					
express_openid_connect					
Session Fixation	09-Dec-21	6.8	Express OpenID Connect is express JS middleware implementing sign on for Express web apps using OpenID Connect. Versions before and including `2.5.1` do not regenerate the session id and session cookie when user logs in. This behavior opens up the application to various session fixation vulnerabilities. Versions `2.5.2` contains a patch for this issue. **CVE ID : CVE-2021-41246**	https://github.com/auth0/express-openid-connect/security/advisories/GHSA-7rg2-qxmf-hhx9, https://github.com/auth0/express-openid-connect/commit/5ab67ff2bd84f76674066b5e129b43ab5f2f43	A-AUT-EXPR-201221/30

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				0f	
ays-pro					
secure_copy_content_protection_and_content_locking					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Dec-21	7.5	The Secure Copy Content Protection and Content Locking WordPress plugin before 2.8.2 does not escape the sccp_id parameter of the ays_sccp_results_export_file AJAX action (available to both unauthenticated and authenticated users) before using it in a SQL statement, leading to an SQL injection. **CVE ID : CVE-2021-24931**	N/A	A-AYS-SECU-201221/31
B2evolution					
b2evolution_cms					
Cross-Site Request Forgery (CSRF)	06-Dec-21	6.8	b2evolution CMS v7.2.3 was discovered to contain a Cross-Site Request Forgery (CSRF) via the User login page. This vulnerability allows attackers to escalate privileges. **CVE ID : CVE-2021-31631**	N/A	A-B2E-B2EV-201221/32
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Dec-21	7.5	b2evolution CMS v7.2.3 was discovered to contain a SQL injection vulnerability via the parameter cfqueryparam in the User login section. This vulnerability allows attackers to execute arbitrary code via a crafted input. **CVE ID : CVE-2021-31632**	N/A	A-B2E-B2EV-201221/33
Barracuda					
network_access_client					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	01-Dec-21	7.2	Barracuda Network Access Client before 5.2.2 creates a Temporary File in a Directory with Insecure Permissions. This file is executed with SYSTEM privileges when an unprivileged user performs a repair operation. **CVE ID : CVE-2021-42711**	N/A	A-BAR-NETW-201221/34
bookly_project					
bookly					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-21	3.5	The WordPress Online Booking and Scheduling Plugin WordPress plugin before 20.3.1 does not escape the Staff Full Name field before outputting it back in a page, which could lead to a Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24930**	N/A	A-BOO-BOOK-201221/35
bookstackapp					
bookstack					
Cross-Site Request Forgery (CSRF)	02-Dec-21	4	bookstack is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-3944**	https://github.com/bookstackapp/bookstack/commit/88e6f93abf54192a69cc8080e0dc6516ee68ccbb, https://huntr.dev/bounties/65551490-5ade-49aa-8b8d-274c2ca9fdc	A-BOO-BOOK-201221/36

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				9	
bosch					
access_professional_edition					
Improper Handling of Exceptional Conditions	08-Dec-21	5	An unauthenticated attacker is able to send a special HTTP request, that causes a service to crash. In case of a standalone VRM or BVMS with VRM installation this crash also opens the possibility to send further unauthenticated commands to the service. On some products the interface is only local accessible lowering the CVSS base score. For a list of modified CVSS scores, please see the official Bosch Advisory Appendix chapter Modified CVSS Scores for CVE-2021-23859 **CVE ID : CVE-2021-23859**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	A-BOS-ACCE-201221/37
bosch_video_management_system					
Improper Handling of Exceptional Conditions	08-Dec-21	5	An unauthenticated attacker is able to send a special HTTP request, that causes a service to crash. In case of a standalone VRM or BVMS with VRM installation this crash also opens the possibility to send further unauthenticated commands to the service. On some products the interface is only local accessible lowering the CVSS base score. For a list of modified CVSS scores, please see the official Bosch Advisory Appendix chapter	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	A-BOS-BOSC-201221/38

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modified CVSS Scores for CVE-2021-23859 **CVE ID : CVE-2021-23859**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	An error in a page handler of the VRM may lead to a reflected cross site scripting (XSS) in the web-based interface. To exploit this vulnerability an attack must be able to modify the HTTP header that is sent. This issue also affects installations of the DIVAR IP and BVMS with VRM installed. **CVE ID : CVE-2021-23860**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	A-BOS-BOSC-201221/39
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-21	5.5	By executing a special command, an user with administrative rights can get access to extended debug functionality on the VRM allowing an impact on integrity or availability of the installed software. This issue also affects installations of the DIVAR IP and BVMS with VRM installed. **CVE ID : CVE-2021-23861**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	A-BOS-BOSC-201221/40
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-21	9	A crafted configuration packet sent by an authenticated administrative user can be used to execute arbitrary commands in system context. This issue also affects installations of the VRM, DIVAR IP, BVMS with VRM installed, the VIDEOJET decoder (VJD-7513 and VJD-8000). **CVE ID : CVE-2021-23862**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	A-BOS-BOSC-201221/41

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
building_integration_system					
Improper Handling of Exceptional Conditions	08-Dec-21	5	An unauthenticated attacker is able to send a special HTTP request, that causes a service to crash. In case of a standalone VRM or BVMS with VRM installation this crash also opens the possibility to send further unauthenticated commands to the service. On some products the interface is only local accessible lowering the CVSS base score. For a list of modified CVSS scores, please see the official Bosch Advisory Appendix chapter Modified CVSS Scores for CVE-2021-23859 **CVE ID : CVE-2021-23859**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	A-BOS-BUIL-201221/42
video_recording_manager					
Improper Handling of Exceptional Conditions	08-Dec-21	5	An unauthenticated attacker is able to send a special HTTP request, that causes a service to crash. In case of a standalone VRM or BVMS with VRM installation this crash also opens the possibility to send further unauthenticated commands to the service. On some products the interface is only local accessible lowering the CVSS base score. For a list of modified CVSS scores, please see the official Bosch Advisory Appendix chapter Modified CVSS Scores for CVE-2021-23859	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	A-BOS-VIDE-201221/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-23859		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	An error in a page handler of the VRM may lead to a reflected cross site scripting (XSS) in the web-based interface. To exploit this vulnerability an attack must be able to modify the HTTP header that is sent. This issue also affects installations of the DIVAR IP and BVMS with VRM installed. **CVE ID : CVE-2021-23860**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	A-BOS-VIDE-201221/44
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-21	5.5	By executing a special command, an user with administrative rights can get access to extended debug functionality on the VRM allowing an impact on integrity or availability of the installed software. This issue also affects installations of the DIVAR IP and BVMS with VRM installed. **CVE ID : CVE-2021-23861**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	A-BOS-VIDE-201221/45
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-21	9	A crafted configuration packet sent by an authenticated administrative user can be used to execute arbitrary commands in system context. This issue also affects installations of the VRM, DIVAR IP, BVMS with VRM installed, the VIDEOJET decoder (VJD-7513 and VJD-8000). **CVE ID : CVE-2021-23862**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	A-BOS-VIDE-201221/46
video_recording_manager_exporter					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	08-Dec-21	5	An unauthenticated attacker is able to send a special HTTP request, that causes a service to crash. In case of a standalone VRM or BVMS with VRM installation this crash also opens the possibility to send further unauthenticated commands to the service. On some products the interface is only local accessible lowering the CVSS base score. For a list of modified CVSS scores, please see the official Bosch Advisory Appendix chapter Modified CVSS Scores for CVE-2021-23859 **CVE ID : CVE-2021-23859**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	A-BOS-VIDE-201221/47
Broadcom					
ca_network_flow_analysis					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-21	4	CA Network Flow Analysis (NFA) 21.2.1 and earlier contain a SQL injection vulnerability in the NFA web application, due to insufficient input validation, that could potentially allow an authenticated user to access sensitive data. **CVE ID : CVE-2021-44050**	https://support.broadcom.com/external/content/security-advisories/CA20211201-01-Security-Notice-for-CA-Network-Flow-Analysis/19689	A-BRO-CA_N-201221/48
browser_and_operating_system_finder_project					
browser_and_operating_system_finder					
Cross-Site Request Forgery	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in Browser and Operating	N/A	A-BRO-BROW-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			System Finder versions prior to 1.2 allows a remote unauthenticated attacker to hijack the authentication of an administrator via unspecified vectors. **CVE ID : CVE-2021-20851**		201221/49
Bundler					
bundler					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	08-Dec-21	9.3	`Bundler` is a package for managing application dependencies in Ruby. In `bundler` versions before 2.2.33, when working with untrusted and apparently harmless `Gemfile`'s, it is not expected that they lead to execution of external code, unless that's explicit in the ruby code inside the `Gemfile` itself. However, if the `Gemfile` includes `gem` entries that use the `git` option with invalid, but seemingly harmless, values with a leading dash, this can be false. To handle dependencies that come from a Git repository instead of a registry, Bundler uses various commands, such as `git clone`. These commands are being constructed using user input (e.g. the repository URL). When building the commands, Bundler versions before 2.2.33 correctly avoid Command Injection vulnerabilities by passing an array of arguments instead of	https://github.com/rubygems/rubygems/commit/a4f2f8ac17e6ce81c689527a8b6f14381060d95f, https://github.com/rubygems/rubygems/security/advisories/GHSA-fj7f-vq84-fh43, https://github.com/rubygems/rubygems/pull/5142	A-BUN-BUND-201221/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a command string. However, there is the possibility that a user input starts with a dash (`-`) and is therefore treated as an optional argument instead of a positional one. This can lead to Code Execution because some of the commands have options that can be leveraged to run arbitrary executables. Since this value comes from the `Gemfile` file, it can contain any character, including a leading dash. To exploit this vulnerability, an attacker has to craft a directory containing a `Gemfile` file that declares a dependency that is located in a Git repository. This dependency has to have a Git URL in the form of `-u./payload`. This URL will be used to construct a Git clone command but will be interpreted as the upload-pack argument. Then this directory needs to be shared with the victim, who then needs to run a command that evaluates the Gemfile, such as `bundle lock`, inside. This vulnerability can lead to Arbitrary Code Execution, which could potentially lead to the takeover of the system. However, the exploitability is very low, because it requires a lot of user interaction. Bundler 2.2.33 has patched this problem by inserting `--`		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as an argument before any positional arguments to those Git commands that were affected by this issue. Regardless of whether users can upgrade or not, they should review any untrustred `Gemfile`'s before running any `bundler` commands that may read them, since they can contain arbitrary ruby code. **CVE ID : CVE-2021-43809**		
c2fo					
comb					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	10-Dec-21	7.5	All versions of package comb are vulnerable to Prototype Pollution via the deepMerge() function. **CVE ID : CVE-2021-23561**	https://snyk.io/vuln/SNYK-JS-COMB-1730083	A-C2F-COMB-201221/51
Calibre-ebook					
calibre					
Allocation of Resources Without Limits or Throttling	07-Dec-21	5	calibre before 5.32.0 contains a regular expression that is vulnerable to ReDoS (Regular Expression Denial of Service) in html_preprocess_rules in ebooks/conversion/preprocess.py. **CVE ID : CVE-2021-44686**	https://bugs.launchpad.net/calibre/+bug/1951979, https://github.com/kovidgoyal/calibre/compare/v5.31.1...v5.32.0	A-CAL-CALI-201221/52
Chamilo					
chamilo					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	4.3	chamilo-lms v1.11.14 is affected by a Cross Site Scripting (XSS) vulnerability in /plugin/jcapture/applet.php if an attacker passes a message hex2bin in the cookie. **CVE ID : CVE-2021-43687**	N/A	A-CHA-CHAM-201221/53
chamilo_lms					
Improper Control of Generation of Code ('Code Injection')	03-Dec-21	6	A remote code execution (RCE) vulnerability in course_intro_pdf_import.php of Chamilo LMS v1.11.x allows authenticated attackers to execute arbitrary code via a crafted .htaccess file. **CVE ID : CVE-2021-35413**	https://github.com/chamilo/chamilo-lms/commit/905a21037ebc9bc5369f0fb380177cb56f496f5c, https://github.com/chamilo/chamilo-lms/commit/2e5c004b57d551678a1815500ef91524ba7bb757	A-CHA-CHAM-201221/54
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Dec-21	7.5	Chamilo LMS v1.11.x was discovered to contain a SQL injection via the doc parameter in main/plagiarism/compilatio/upload.php. **CVE ID : CVE-2021-35414**	https://support.chamilo.org/projects/1/wiki/Security_issues#Issue-59-2021-05-13-High-impact-low-risk-Unauthenticated-SQL-injection-vulnerability-when-a-	A-CHA-CHAM-201221/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				module-is-enabled	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Dec-21	3.5	A stored cross-site scripting (XSS) vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the course "Title" and "Content" fields. **CVE ID : CVE-2021-35415**	https://github.com/andrejspuler/writeups/tree/main/chamilo-lms#multiple-stored-cross-site-scripting-vulnerabilities, https://support.chamilo.org/projects/1/wiki/Security_issues#Issue-63-2021-05-14-Low-impact-moderate-risk-XSS-in-course-documents	A-CHA-CHAM-201221/56
Citrix					
gateway					
Uncontrolled Resource Consumption	07-Dec-21	4.3	A unauthenticated denial of service vulnerability exists in Citrix ADC <13.0-83.27, <12.1-63.22 and 11.1-65.23 when configured as a VPN (Gateway) or AAA virtual server could allow an attacker to cause a temporary disruption of the Management GUI, Nitro API, and RPC communication. **CVE ID : CVE-2021-22955**	https://support.citrix.com/article/CTX330728	A-CIT-GATE-201221/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	07-Dec-21	4.3	An uncontrolled resource consumption vulnerability exists in Citrix ADC <13.0-83.27, <12.1-63.22 and 11.1-65.23 that could allow an attacker with access to NSIP or SNIP with management interface access to cause a temporary disruption of the Management GUI, Nitro API, and RPC communication. **CVE ID : CVE-2021-22956**	https://support.citrix.com/article/CTX330728	A-CIT-GATE-201221/58
sd-wan					
Uncontrolled Resource Consumption	07-Dec-21	4.3	An uncontrolled resource consumption vulnerability exists in Citrix ADC <13.0-83.27, <12.1-63.22 and 11.1-65.23 that could allow an attacker with access to NSIP or SNIP with management interface access to cause a temporary disruption of the Management GUI, Nitro API, and RPC communication. **CVE ID : CVE-2021-22956**	https://support.citrix.com/article/CTX330728	A-CIT-SD-W-201221/59
cloverdx					
cloverdx					
Improper Restriction of XML External Entity Reference	01-Dec-21	6.8	CloverDX Server before 5.11.2 and and 5.12.x before 5.12.1 allows XXE during configuration import. **CVE ID : CVE-2021-42776**	https://support1.cloverdx.com/hc/en-us/articles/441112542901 0, https://support.cloverdx.com/releases/	A-CLO-CLOV-201221/60
Codesys					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
development_system					
Improper Certificate Validation	01-Dec-21	5.8	Affected versions of CODESYS Git in Versions prior to V1.1.0.0 lack certificate validation in HTTPS handshakes. CODESYS Git does not implement certificate validation by default, so it does not verify that the server provides a valid and trusted HTTPS certificate. Since the certificate of the server to which the connection is made is not properly verified, the server connection is vulnerable to a man-in-the-middle attack. **CVE ID : CVE-2021-34599**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16959&token=3ce11e44a3277c4520d732ea2e630f2e06bd46ff&download	A-COD-DEVE-201221/61
git					
Improper Certificate Validation	01-Dec-21	5.8	Affected versions of CODESYS Git in Versions prior to V1.1.0.0 lack certificate validation in HTTPS handshakes. CODESYS Git does not implement certificate validation by default, so it does not verify that the server provides a valid and trusted HTTPS certificate. Since the certificate of the server to which the connection is made is not properly verified, the server connection is vulnerable to a man-in-the-middle attack. **CVE ID : CVE-2021-34599**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16959&token=3ce11e44a3277c4520d732ea2e630f2e06bd46ff&download	A-COD-GIT-201221/62
comment_engine_pro_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
comment_engine_pro					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-21	3.5	Stored Cross-Site Scripting (XSS) vulnerability discovered in WordPress Comment Engine Pro plugin (versions <= 1.0), could be exploited by users with Editor or higher role. **CVE ID : CVE-2021-36911**	https://wordpress.org/plugins/comment-engine-pro/	A-COM-COMM-201221/63
couchbase					
sync_gateway					
Exposure of Sensitive Information to an Unauthorized Actor	07-Dec-21	5.5	An issue was discovered in Couchbase Sync Gateway 2.7.0 through 2.8.2. The bucket credentials used to read and write data in Couchbase Server were insecurely being stored in the metadata within sync documents written to the bucket. Users with read access could use these credentials to obtain write access. (This issue does not affect clusters where Sync Gateway is authenticated with X.509 client certificates. This issue also does not affect clusters where shared bucket access is not enabled on Sync Gateway.) **CVE ID : CVE-2021-43963**	https://www.couchbase.com/alerts	A-COU-SYNC-201221/64
Craftercms					
crafter_cms					
Improper Control of Dynamically-Managed	02-Dec-21	6.5	Authenticated users with Administrator or Developer roles may execute OS commands by SPEL	https://docs.craftercms.org/en/3.1/security/adviso	A-CRA-CRAF-201221/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Code Resources			Expression in Spring beans. SPEL Expression does not have security restrictions, which will cause attackers to execute arbitrary commands remotely (RCE). **CVE ID : CVE-2021-23258**	ry.html#cv-2021120101	
Improper Control of Dynamically-Managed Code Resources	02-Dec-21	6.5	Authenticated users with Administrator or Developer roles may execute OS commands by Groovy Script which uses Groovy lib to render a webpage. The groovy script does not have security restrictions, which will cause attackers to execute arbitrary commands remotely(RCE). **CVE ID : CVE-2021-23259**	https://docs.craftercms.org/en/3.1/security/advisory.html#cv-2021120102	A-CRA-CRAF-201221/66
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-21	3.5	Authenticated users with Site roles may inject XSS scripts via file names that will execute in the browser for this and other users of the same site. **CVE ID : CVE-2021-23260**	https://docs.craftercms.org/en/3.1/security/advisory.html#cv-2021120103	A-CRA-CRAF-201221/67
N/A	02-Dec-21	4	Authenticated administrators may override the system configuration file and cause a denial of service. **CVE ID : CVE-2021-23261**	https://docs.craftercms.org/en/3.1/security/advisory.html#cv-2021120104	A-CRA-CRAF-201221/68
Improper Control of Dynamically-Managed Code Resources	02-Dec-21	6.5	Authenticated administrators may modify the main YAML configuration file and load a Java class resulting in RCE. **CVE ID : CVE-2021-23262**	https://docs.craftercms.org/en/3.1/security/advisory.html#cv-2021120105	A-CRA-CRAF-201221/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	02-Dec-21	5	Unauthenticated remote attackers can read textual content via FreeMarker including files /scripts/*, /templates/* and some of the files in /.git/* (non-binary). **CVE ID : CVE-2021-23263**	https://docs.craftercms.org/en/3.1/security/advisory.html#cv-2021120106	A-CRA-CRAF-201221/70
Exposure of Resource to Wrong Sphere	02-Dec-21	6.4	Installations, where crafter-search is not protected, allow unauthenticated remote attackers to create, view, and delete search indexes. **CVE ID : CVE-2021-23264**	https://docs.craftercms.org/en/3.1/security/advisory.html#cv-2021120107	A-CRA-CRAF-201221/71
cybonet					
mail_secure					
Unrestricted Upload of File with Dangerous Type	08-Dec-21	9	PineApp - Mail Secure - The attacker must be logged in as a user to the Pineapp system. The attacker exploits the vulnerable nicUpload.php file to upload a malicious file,Thus taking over the server and running remote code. **CVE ID : CVE-2021-36719**	N/A	A-CYB-MAIL-201221/72
Dart					
dart_software_development_kit					
Exposure of Resource to Wrong Sphere	09-Dec-21	6	When using the dart pub publish command to publish a package to a third-party package server, the request would be authenticated with an oauth2 access_token that is valid for publishing on pub.dev. Using these obtained credentials, an attacker can impersonate the user on pub.dev. We recommend	https://github.com/dart-lang/sdk/blob/main/CHANGELOG.md, https://github.com/dart-lang/sdk/security/advisories/GHSA-r32f-vhjp-	A-DAR-DART-201221/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			upgrading past https://github.com/dart-lang/sdk/commit/d787e78d21e12ec1ef712d229940b1172aafcdf8 or beyond version 2.15.0 **CVE ID : CVE-2021-22568**	qhj7, https://github.com/dart-lang/sdk/commit/d787e78d21e12ec1ef712d229940b1172aafcdf8	
deltaww					
cncsoft					
Stack-based Buffer Overflow	09-Dec-21	6.8	Delta Electronics CNCSoft Versions 1.01.30 and prior are vulnerable to a stack-based buffer overflow, which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2021-43982**	N/A	A-DEL-CNCS-201221/74
devise_masquerade_project					
devise_masquerade					
N/A	07-Dec-21	6.8	The devise_masquerade gem before 1.3 allows certain attacks when a password's salt is unknown. An application that uses this gem to let administrators masquerade/impersonate users loses one layer of security protection compared to a situation where Devise (without this extension) is used. If the server-side secret_key_base value became publicly known (for instance if it is committed to a public repository by mistake), there are still other protections in place that prevent an attacker from	N/A	A-DEV-DEVI-201221/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impersonating any user on the site. When masquerading is not used in a plain Devise application, one must know the password salt of the target user if one wants to encrypt and sign a valid session cookie. When devise_masquerade is used, however, an attacker can decide which user the "back" action will go back to without knowing that user's password salt and simply knowing the user ID, by manipulating the session cookie and pretending that a user is already masqueraded by an administrator. **CVE ID : CVE-2021-28680**		
digipas					
egeetouch_3rd_generation_travel_padlock					
Missing Encryption of Sensitive Data	02-Dec-21	2.9	An issue was discovered in the eGeeTouch 3rd Generation Travel Padlock application for Android. The lock sends a pairing code before each operation (lock or unlock) activated via the companion app. The code is sent unencrypted, allowing any attacker with the same app (either Android or iOS) to add the lock and take complete control. For successful exploitation, the attacker must be able to touch the lock's power button, and must be able to capture BLE network	N/A	A-DIG-EGEE-201221/76

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			communication. **CVE ID : CVE-2021-44518**		
discourse					
discourse					
Exposure of Sensitive Information to an Unauthorized Actor	01-Dec-21	3.5	Discourse is an open source discussion platform. In affected versions a vulnerability affects users of tag groups who use the "Tags are visible only to the following groups" feature. A tag group may only allow a certain group (e.g. staff) to view certain tags. Users who were tracking or watching the tags via /preferences/tags, then have their staff status revoked will still see notifications related to the tag, but will not see the tag on each topic. This issue has been patched in stable version 2.7.11. Users are advised to upgrade as soon as possible. **CVE ID : CVE-2021-43792**	https://github.com/discourse/discourse/commit/cdaf7f4bb3ec268238e4c29a14bb73fad56574b4, https://github.com/discourse/discourse/security/advisories/GHSA-pq2x-vq37-8522	A-DIS-DISC-201221/77
Improper Privilege Management	01-Dec-21	4	Discourse is an open source discussion platform. In affected versions a vulnerability in the Polls feature allowed users to vote multiple times in a single-option poll. The problem is patched in the latest tests-passed, beta and stable versions of Discourse **CVE ID : CVE-2021-43793**	https://github.com/discourse/discourse/security/advisories/GHSA-jq7h-44vc-h6qx, https://github.com/discourse/discourse/commit/0c6b9df77bac9c6f7c7e2ea	A-DIS-DISC-201221/78

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				df6fe100064afdeab, https://github.com/discourse/discourse/commit/1d0faedfbc3a8b77b971dc70d25e30791dbb6e0b	
Externally Controlled Reference to a Resource in Another Sphere	01-Dec-21	5	Discourse is an open source discussion platform. In affected versions an attacker can poison the cache for anonymous (i.e. not logged in) users, such that the users are shown a JSON blob instead of the HTML page. This can lead to a partial denial-of-service. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. **CVE ID : CVE-2021-43794**	https://github.com/discourse/discourse/security/advisories/GHSA-249g-pc77-65hp, https://github.com/discourse/discourse/commit/2da0001965c6d8632d723c46ea5df9f22a1a23f1	A-DIS-DISC-201221/79
django-helpdesk_project					
django-helpdesk					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	6.8	django-helpdesk is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-3994**	https://github.com/django-helpdesk/django-helpdesk/commit/a22eb0673fe0b7784f99c6b5fd343b64a6700f06, https://huntr.dev/bounti	A-DJA-DJAN-201221/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				es/be7f211d-4bfd-44fd-91e8-682329906fbd	
Djangoproject					
django					
Improper Authentication	08-Dec-21	7.5	In Django 2.2 before 2.2.25, 3.1 before 3.1.14, and 3.2 before 3.2.10, HTTP requests for URLs with trailing newlines could bypass upstream access control based on URL paths. **CVE ID : CVE-2021-44420**	https://docs.djangoproject.com/en/3.2/releases/security/, https://www.openwall.com/lists/oss-security/2021/12/07/1, https://www.djangoproject.com/weblog/2021/dec/07/security-releases/	A-DJA-DJAN-201221/81
donglify					
donglify					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	Donglify is affected by Buffer Overflow. IOCTL Handler 0x22001B in the Donglify above 1.0.12309 below 1.7.14110 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42994**	N/A	A-DON-DONG-201221/82

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-Dec-21	7.2	Donglify is affected by Integer Overflow. IOCTL Handler 0x22001B in the Donglify above 1.0.12309 below 1.7.14110 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42996**	N/A	A-DON-DONG-201221/83
douco					
douphp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	DouPHP v1.6 was discovered to contain a cross-site scripting (XSS) vulnerability via /admin/cloud.php. **CVE ID : CVE-2021-3370**	N/A	A-DOU-DOUP-201221/84
Dreamreport					
remote_connector					
Unrestricted Upload of File with Dangerous Type	08-Dec-21	6.8	A privilege escalation vulnerability exists in the Remote Server functionality of Dream Report ODS Remote Connector 20.2.16900.0. A specially-crafted command injection can lead to elevated capabilities. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21957**	N/A	A-DRE-REMO-201221/85
dzzoffice					
dzzoffice					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Dec-21	4.3	dzzoffice 2.02.1_SC_UTF8 is affected by a Cross Site Scripting (XSS) vulnerability in explorerfile.php. The output of the exit function is printed for the user via exit(json_encode($return)). **CVE ID : CVE-2021-43673**	N/A	A-DZZ-DZZO-201221/86
Eclipse					
mosquitto					
N/A	01-Dec-21	5	In versions 1.6 to 2.0.11 of Eclipse Mosquitto, an MQTT v5 client connecting with a large number of user-property properties could cause excessive CPU usage, leading to a loss of performance and possible denial of service. **CVE ID : CVE-2021-41039**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=575314	A-ECL-MOSQ-201221/87
Elastic					
apm_agent					
Improper Privilege Management	08-Dec-21	4.4	A local privilege escalation issue was found with the APM Java agent, where a user on the system could attach a malicious file to an application running with the APM Java agent. Using this vector, a malicious or compromised user account could use the agent to run commands at a higher level of permissions than they possess. This vulnerability affects users that have set up the agent via the attacher cli 3, the attach API 2, as well as	https://discuss.elastic.co/t/apm-java-agent-security-update/289627	A-ELA-APM_-201221/88

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users that have enabled the profiling_inferred_spans_enabled option **CVE ID : CVE-2021-37941**		
enterprise_search					
Server-Side Request Forgery (SSRF)	07-Dec-21	4	An information disclosure via GET request server-side request forgery vulnerability was discovered with the Workplace Search Github Enterprise Server integration. Using this vulnerability, a malicious Workplace Search admin could use the GHES integration to view hosts that might not be publicly accessible. **CVE ID : CVE-2021-37940**	https://discuss.elastic.co/t/enterprise-search-7-16-0-security-update/291146	A-ELA-ENTE-201221/89
Elgg					
elgg					
Authorization Bypass Through User-Controlled Key	01-Dec-21	4.3	elgg is vulnerable to Authorization Bypass Through User-Controlled Key **CVE ID : CVE-2021-3964**	https://github.com/elgg/elgg/commit/d9fcad76ee380ea17edd61d13d0f87828ea3f744, https://huntr.dev/bounties/a4df45d6-b739-4299-967f-c960b569383a	A-ELG-ELGG-201221/90
Exposure of Private Personal Information	03-Dec-21	5	elgg is vulnerable to Exposure of Private Personal Information to an Unauthorized Actor	https://github.com/elgg/elgg/commit/572d210e2	A-ELG-ELGG-201221/91

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to an Unauthorized Actor			**CVE ID : CVE-2021-3980**	392f1fdf47ff2f38665372a6535c126, https://hunter.dev/bounties/1f43f11e-4bd8-451f-a244-dc9541cdc0ac	
eltima					
usb_network_gate					
Integer Overflow or Wraparound	07-Dec-21	7.2	Eltima USB Network Gate is affected by Integer Overflow. IOCTL Handler 0x22001B in the USB Network Gate above 7.0.1370 below 9.2.2420 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42987**	N/A	A-ELT-USB_-201221/92
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	Eltima USB Network Gate is affected by Buffer Overflow. IOCTL Handler 0x22001B in the USB Network Gate above 7.0.1370 below 9.2.2420 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42988**	N/A	A-ELT-USB_-201221/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
email_log_project					
email_log					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-21	4.3	The Email Log WordPress plugin before 2.4.8 does not escape the d parameter before outputting it back in an attribute in the Log page, leading to a Reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24924**	N/A	A-EMA-EMAI-201221/94
employee_record_management_system_project					
employee_record_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Dec-21	7.5	SQL Injection vulnerability exists in PHPGURUKUL Employee Record Management System 1.2 via the Email POST parameter in /forgetpassword.php. **CVE ID : CVE-2021-43451**	N/A	A-EMP-EMPL-201221/95
Esri					
arcgis_enterprise					
Exposure of Resource to Wrong Sphere	07-Dec-21	5	An information disclosure vulnerability in the ArcGIS Service Directory in Esri ArcGIS Enterprise versions 10.9.0 and below may allows a remote attacker to view hidden field names in feature layers. This issue may reveal field names, but not not disclose features. **CVE ID : CVE-2021-29115**	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-server-security-2021-update-2-patch-is-now-available	A-ESR-ARCG-201221/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
arcgis_server					
Improper Control of Generation of Code ('Code Injection')	07-Dec-21	4.3	A remote file inclusion vulnerability in the ArcGIS Server help documentation may allow a remote, unauthenticated attacker to inject attacker supplied html into a page. **CVE ID : CVE-2021-29113**	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-server-security-2021-update-2-patch-is-now-available	A-ESR-ARCG-201221/97
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Dec-21	7.5	A SQL injection vulnerability in feature services provided by Esri ArcGIS Server 10.9 and below allows a remote, unauthenticated attacker to impact the confidentiality, integrity and availability of targeted services via specifically crafted queries. **CVE ID : CVE-2021-29114**	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-server-security-2021-update-2-patch-is-now-available	A-ESR-ARCG-201221/98
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-21	4.3	A stored Cross Site Scripting (XSS) vulnerability in Esri ArcGIS Server feature services versions 10.8.1 and 10.9 (only) feature services may allow a remote, unauthenticated attacker to pass and store malicious strings via crafted queries	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-server-	A-ESR-ARCG-201221/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which when accessed could potentially execute arbitrary JavaScript code in the user's browser. **CVE ID : CVE-2021-29116**	security-2021-update-2-patch-is-now-available	
F-secure					
safe					
Improper Restriction of Rendered UI Layers or Frames	10-Dec-21	4.3	A user interface overlay vulnerability was discovered in F-secure SAFE Browser for Android. When user click on a specially crafted seemingly legitimate URL SAFE browser goes into full screen and hides the user interface. A remote attacker can leverage this to perform spoofing attack. **CVE ID : CVE-2021-40834**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40834	A-F-S-SAFE-201221/100
F5					
nginx_modsecurity_waf					
Uncontrolled Recursion	07-Dec-21	5	ModSecurity 3.x through 3.0.5 mishandles excessively nested JSON objects. Crafted JSON objects with nesting tens-of-thousands deep could result in the web server being unable to service legitimate requests. Even a moderately large (e.g., 300KB) HTTP request can occupy one of the	https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/modsecurity-dos-vulnerability-in-json-	A-F5-NGIN-201221/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			limited NGINX worker processes for minutes and consume almost all of the available CPU on the machine. Modsecurity 2 is similarly vulnerable: the affected versions include 2.8.0 through 2.9.4. **CVE ID : CVE-2021-42717**	parsing-cve-2021-42717/	
firefly-iii					
firefly_iii					
Cross-Site Request Forgery (CSRF)	04-Dec-21	4.3	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-4005**	https://huntr.dev/bounties/bf4ef581-325a-492d-a710-14fcb53f00ff, https://github.com/firefly-iii/firefly-iii/commit/03a1601bf343181df9f405dd2109aec483cb7053	A-FIR-FIRE-201221/102
Cross-Site Request Forgery (CSRF)	01-Dec-21	4.3	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-4015**	https://github.com/firefly-iii/firefly-iii/commit/518b4ba5a7a56760902758ae0a2c6a392c2f4d37, https://huntr.dev/bounties/b698d445-602d-4701-961c-dffe6d3009b	A-FIR-FIRE-201221/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1	
flexihub					
flexihub					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	FlexiHub For Windows is affected by Buffer Overflow. IOCTL Handler 0x22001B in the FlexiHub For Windows above 2.0.4340 below 5.3.14268 allows local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42990**	N/A	A-FLE-FLEX-201221/104
Integer Overflow or Wraparound	07-Dec-21	7.2	FlexiHub For Windows is affected by Integer Overflow. IOCTL Handler 0x22001B in the FlexiHub For Windows above 2.0.4340 below 5.3.14268 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42993**	N/A	A-FLE-FLEX-201221/105
Fortinet					
fortiadc					
Use of a Broken or Risky Cryptographic Algorithm	08-Dec-21	2.6	A missing cryptographic steps vulnerability in the function that encrypts users' LDAP and RADIUS credentials in FortiSandbox before 4.0.1, FortiWeb before 6.3.12, FortiADC before 6.2.1,	https://fortiguard.com/advisory/FG-IR-20-222	A-FOR-FORT-201221/106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FortiMail 7.0.1 and earlier may allow an attacker in possession of the password store to compromise the confidentiality of the encrypted secrets. **CVE ID : CVE-2021-32591**		
fortianalyzer					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	4.6	A buffer overflow [CWE-121] in the TFTP client library of FortiOS before 6.4.7 and FortiOS 7.0.0 through 7.0.2, may allow an authenticated local attacker to achieve arbitrary code execution via specially crafted command line arguments. **CVE ID : CVE-2021-42757**	https://fortiguard.com/advisory/FG-IR-21-173	A-FOR-FORT-201221/107
fortiauthenticator					
Exposure of Sensitive Information to an Unauthorized Actor	08-Dec-21	4.3	A exposure of sensitive information to an unauthorized actor in Fortinet FortiAuthenticator version 6.4.0, version 6.3.2 and below, version 6.2.1 and below, version 6.1.2 and below, version 6.0.7 to 6.0.1 allows attacker to duplicate a target LDAP user 2 factors authentication token via crafted HTTP requests. **CVE ID : CVE-2021-43067**	https://fortiguard.com/advisory/FG-IR-21-211	A-FOR-FORT-201221/108
Improper Authentication	09-Dec-21	5.5	A improper authentication in Fortinet FortiAuthenticator version 6.4.0 allows user to bypass the second factor of authentication via a RADIUS login portal.	https://fortiguard.com/advisory/FG-IR-21-212	A-FOR-FORT-201221/109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-43068		
forticlient					
Incorrect Authorizatio n	09-Dec-21	5	An improper authorization vulnerabiltiy [CWE-285] in FortiClient Windows versions 7.0.0 and 6.4.6 and below and 6.2.8 and below may allow an unauthenticated attacker to bypass the webfilter control via modifying the session-id paramater. **CVE ID : CVE-2021-36167**	https://forti guard.com/a dvisory/FG-IR-20-127	A-FOR-FORT-201221/110
N/A	09-Dec-21	4.9	A improper control of a resource through its lifetime in Fortinet FortiClientWindows version 6.4.1 and 6.4.0, version 6.2.9 and below, version 6.0.10 and below allows attacker to cause a complete denial of service of its components via changes of directory access permissions. **CVE ID : CVE-2021-43204**	https://forti guard.com/a dvisory/FG-IR-21-167	A-FOR-FORT-201221/111
Uncontrolled Search Path Element	01-Dec-21	6.9	An unsafe search path vulnerability in FortiClientWindows 7.0.0, 6.4.6 and below, 6.2.x, 6.0.x and FortiClientEMS 7.0.0, 6.4.6 and below, 6.2.x, 6.0.x may allow an attacker to perform a DLL Hijack attack on affected devices via a malicious OpenSSL engine library in the search path. **CVE ID : CVE-2021-32592**	https://forti guard.com/a dvisory/FG-IR-21-088	A-FOR-FORT-201221/112
forticlient_enterprise_management_server					
Missing	09-Dec-21	4	A missing encryption of	https://forti	A-FOR-FORT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Encryption of Sensitive Data			sensitive data in Fortinet FortiClientEMS version 7.0.1 and below, version 6.4.4 and below allows attacker to information disclosure via inspecting browser decrypted data **CVE ID : CVE-2021-36189**	guard.com/advisory/FG-IR-21-140	201221/113
Authentication Bypass by Capture-replay	08-Dec-21	6.4	An authentication bypass by capture-replay vulnerability [CWE-294] in FortiClient EMS versions 7.0.1 and below and 6.4.4 and below may allow an unauthenticated attacker to impersonate an existing user by intercepting and re-using valid SAML authentication messages. **CVE ID : CVE-2021-41030**	https://fortiguard.com/advisory/FG-IR-21-192	A-FOR-FORT-201221/114
Uncontrolled Search Path Element	01-Dec-21	6.9	An unsafe search path vulnerability in FortiClientWindows 7.0.0, 6.4.6 and below, 6.2.x, 6.0.x and FortiClientEMS 7.0.0, 6.4.6 and below, 6.2.x, 6.0.x may allow an attacker to perform a DLL Hijack attack on affected devices via a malicious OpenSSL engine library in the search path. **CVE ID : CVE-2021-32592**	https://fortiguard.com/advisory/FG-IR-21-088	A-FOR-FORT-201221/115
fortimail					
Use of a Broken or Risky Cryptographic Algorithm	08-Dec-21	2.6	A missing cryptographic steps vulnerability in the function that encrypts users' LDAP and RADIUS credentials in FortiSandbox before 4.0.1, FortiWeb before 6.3.12, FortiADC before 6.2.1,	https://fortiguard.com/advisory/FG-IR-20-222	A-FOR-FORT-201221/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FortiMail 7.0.1 and earlier may allow an attacker in possession of the password store to compromise the confidentiality of the encrypted secrets. **CVE ID : CVE-2021-32591**		
fortimanager					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	4.6	A buffer overflow [CWE-121] in the TFTP client library of FortiOS before 6.4.7 and FortiOS 7.0.0 through 7.0.2, may allow an authenticated local attacker to achieve arbitrary code execution via specially crafted command line arguments. **CVE ID : CVE-2021-42757**	https://fortiguard.com/advisory/FG-IR-21-173	A-FOR-FORT-201221/117
fortinac					
Improper Privilege Management	08-Dec-21	7.2	A privilege escalation vulnerability in FortiNAC versions 8.8.8 and below and 9.1.2 and below may allow an admin user to escalate the privileges to root via the sudo command. **CVE ID : CVE-2021-41021**	https://fortiguard.com/advisory/FG-IR-21-182	A-FOR-FORT-201221/118
Incorrect Permission Assignment for Critical Resource	09-Dec-21	7.2	A incorrect permission assignment for critical resource in Fortinet FortiNAC version 9.2.0, version 9.1.3 and below, version 8.8.9 and below allows attacker to gain higher privileges via the access to sensitive system data. **CVE ID : CVE-2021-43065**	https://fortiguard.com/advisory/FG-IR-21-178	A-FOR-FORT-201221/119
fortiproxy					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-21	5	A relative path traversal [CWE-23] vulnerabiltiy in FortiOS versions 7.0.0 and 7.0.1 and FortiProxy verison 7.0.0 may allow an unauthenticated, unauthorized attacker to inject path traversal character sequences to disclose sensitive information of the server via the GET request of the login page. **CVE ID : CVE-2021-41024**	https://fortiguard.com/advisory/FG-IR-21-181	A-FOR-FORT-201221/120
Insufficient Verification of Data Authenticity	08-Dec-21	5.1	An insufficient verification of data authenticity vulnerability (CWE-345) in the user interface of FortiProxy verison 2.0.3 and below, 1.2.11 and below and FortiGate verison 7.0.0, 6.4.6 and below, 6.2.9 and below of SSL VPN portal may allow a remote, unauthenticated attacker to conduct a cross-site request forgery (CSRF) attack . Only SSL VPN in web mode or full mode are impacted by this vulnerability. **CVE ID : CVE-2021-26103**	https://fortiguard.com/advisory/FG-IR-20-158	A-FOR-FORT-201221/121
Improper Privilege Management	08-Dec-21	4.6	An improper access control vulnerability [CWE-284] in FortiOS autod daemon 7.0.0, 6.4.6 and below, 6.2.9 and below, 6.0.12 and below and FortiProxy 2.0.1 and below, 1.2.9 and below may allow an authenticated low-privileged attacker to escalate their privileges to super_admin via	https://fortiguard.com/advisory/FG-IR-20-131	A-FOR-FORT-201221/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a specific crafted configuration of fabric automation CLI script and auto-script features. **CVE ID : CVE-2021-26110**		
fortisandbox					
Use of a Broken or Risky Cryptographic Algorithm	08-Dec-21	2.6	A missing cryptographic steps vulnerability in the function that encrypts users' LDAP and RADIUS credentials in FortiSandbox before 4.0.1, FortiWeb before 6.3.12, FortiADC before 6.2.1, FortiMail 7.0.1 and earlier may allow an attacker in possession of the password store to compromise the confidentiality of the encrypted secrets. **CVE ID : CVE-2021-32591**	https://fortiguard.com/advisory/FG-IR-20-222	A-FOR-FORT-201221/123
fortiweb					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-21	6.5	Multiple improper neutralization of special elements used in a command vulnerabilities [CWE-77] in FortiWeb management interface 6.4.1 and below, 6.3.15 and below, 6.2.5 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. **CVE ID : CVE-2021-36180**	https://fortiguard.com/advisory/FG-IR-21-120	A-FOR-FORT-201221/124
Improper Neutralization of Input During Web	08-Dec-21	4.3	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet	https://fortiguard.com/advisory/FG-IR-21-118	A-FOR-FORT-201221/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			FortiWeb version 6.4.1 and below, 6.3.15 and below allows attacker to execute unauthorized code or commands via crafted GET parameters in requests to login and error handlers **CVE ID : CVE-2021-36188**		
Externally Controlled Reference to a Resource in Another Sphere	08-Dec-21	6.5	A unintended proxy or intermediary ('confused deputy') in Fortinet FortiWeb version 6.4.1 and below, 6.3.15 and below allows an unauthenticated attacker to access protected hosts via crafted HTTP requests. **CVE ID : CVE-2021-36190**	https://fortiguard.com/advisory/FG-IR-21-123	A-FOR-FORT-201221/126
URL Redirection to Untrusted Site ('Open Redirect')	08-Dec-21	5.8	A url redirection to untrusted site ('open redirect') in Fortinet FortiWeb version 6.4.1 and below, 6.3.15 and below allows attacker to use the device as proxy via crafted GET parameters in requests to error handlers **CVE ID : CVE-2021-36191**	https://fortiguard.com/advisory/FG-IR-21-133	A-FOR-FORT-201221/127
Out-of-bounds Write	09-Dec-21	6.5	Multiple stack-based buffer overflows in the API controllers of FortiWeb 6.4.1, 6.4.0, and 6.3.0 through 6.3.15 may allow an authenticated attacker to achieve arbitrary code execution via specially crafted requests. **CVE ID : CVE-2021-36194**	https://fortiguard.com/advisory/FG-IR-21-152	A-FOR-FORT-201221/128
Improper Neutralization of Special	08-Dec-21	9	Multiple command injection vulnerabilities in the command line interpreter of	https://fortiguard.com/advisory/FG-	A-FOR-FORT-201221/129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			FortiWeb versions 6.4.1, 6.4.0, 6.3.0 through 6.3.15, 6.2.0 through 6.2.6, and 6.1.0 through 6.1.2 may allow an authenticated attacker to execute arbitrary commands on the underlying system shell via specially crafted command arguments. **CVE ID : CVE-2021-36195**	IR-21-157	
Incorrect Authorization	08-Dec-21	5	An improper access control vulnerability [CWE-284] in FortiWeb versions 6.4.1 and below and 6.3.15 and below in the Report Browse section of Log & Report may allow an unauthorized and unauthenticated user to access the Log reports via their URLs. **CVE ID : CVE-2021-41013**	https://fortiguard.com/advisory/FG-IR-21-138	A-FOR-FORT-201221/130
Uncontrolled Resource Consumption	08-Dec-21	5	A uncontrolled resource consumption in Fortinet FortiWeb version 6.4.1 and below, 6.3.15 and below allows an unauthenticated attacker to make the httpsd daemon unresponsive via huge HTTP packets **CVE ID : CVE-2021-41014**	https://fortiguard.com/advisory/FG-IR-21-131	A-FOR-FORT-201221/131
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiWeb version 6.4.1 and below, 6.3.15 and below allows attacker to execute unauthorized code or commands via crafted HTTP	https://fortiguard.com/advisory/FG-IR-21-139	A-FOR-FORT-201221/132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests to SAML login handler **CVE ID : CVE-2021-41015**		
Out-of-bounds Write	08-Dec-21	6.5	Multiple heap-based buffer overflow vulnerabilities in some web API controllers of FortiWeb 6.4.1, 6.4.0, and 6.3.0 through 6.3.15 may allow a remote authenticated attacker to execute arbitrary code or commands via specifically crafted HTTP requests. **CVE ID : CVE-2021-41017**	https://fortiguard.com/advisory/FG-IR-21-160	A-FOR-FORT-201221/133
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Dec-21	7.5	Multiple vulnerabilities in the authentication mechanism of confd in FortiWeb versions 6.4.1, 6.4.0, 6.3.0 through 6.3.15, 6.2.0 through 6.2.6, 6.1.0 through 6.1.2, 6.0.0 thorugh 6.0.7, including an instance of concurrent execution using shared resource with improper synchronization and one of authentication bypass by capture-replay, may allow a remote unauthenticated attacker to circumvent the authentication process and authenticate as a legitimate cluster peer. **CVE ID : CVE-2021-41025**	https://fortiguard.com/advisory/FG-IR-21-130	A-FOR-FORT-201221/134
Out-of-bounds Write	08-Dec-21	4.6	A stack-based buffer overflow in Fortinet FortiWeb version 6.4.1 and 6.4.0, allows an authenticated attacker to execute unauthorized code or commands via crafted	https://fortiguard.com/advisory/FG-IR-21-134	A-FOR-FORT-201221/135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certificates loaded into the device. **CVE ID : CVE-2021-41027**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	4.6	A buffer overflow [CWE-121] in the TFTP client library of FortiOS before 6.4.7 and FortiOS 7.0.0 through 7.0.2, may allow an authenticated local attacker to achieve arbitrary code execution via specially crafted command line arguments. **CVE ID : CVE-2021-42757**	https://fortiguard.com/advisory/FG-IR-21-173	A-FOR-FORT-201221/136
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiWeb version 6.4.1 and 6.4.0, version 6.3.15 and below, version 6.2.6 and below allows attacker to execute unauthorized code or commands via crafted HTTP GET requests to the login webpage. **CVE ID : CVE-2021-43063**	https://fortiguard.com/advisory/FG-IR-21-122	A-FOR-FORT-201221/137
URL Redirection to Untrusted Site ('Open Redirect')	08-Dec-21	5.8	A url redirection to untrusted site ('open redirect') in Fortinet FortiWeb version 6.4.1 and 6.4.0, version 6.3.15 and below, version 6.2.6 and below allows attacker to use the device as a proxy and reach external or protected hosts via redirection handlers. **CVE ID : CVE-2021-43064**	https://fortiguard.com/advisory/FG-IR-21-168	A-FOR-FORT-201221/138
Out-of-bounds	09-Dec-21	6.5	A heap-based buffer overflow in Fortinet FortiWeb version	https://fortiguard.com/a	A-FOR-FORT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			6.4.1 and 6.4.0, version 6.3.15 and below, version 6.2.6 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests to the LogReport API controller. **CVE ID : CVE-2021-43071**	dvisory/FG-IR-21-188	201221/139
Use of a Broken or Risky Cryptographic Algorithm	08-Dec-21	2.6	A missing cryptographic steps vulnerability in the function that encrypts users' LDAP and RADIUS credentials in FortiSandbox before 4.0.1, FortiWeb before 6.3.12, FortiADC before 6.2.1, FortiMail 7.0.1 and earlier may allow an attacker in possession of the password store to compromise the confidentiality of the encrypted secrets. **CVE ID : CVE-2021-32591**	https://fortiguard.com/advisory/FG-IR-20-222	A-FOR-FORT-201221/140
fortiwlc					
Incorrect Authorization	08-Dec-21	9	An improper access control vulnerability [CWE-284] in FortiWLC 8.6.1 and below may allow an authenticated and remote attacker with low privileges to execute any command as an admin user with full access rights via bypassing the GUI restrictions. **CVE ID : CVE-2021-42758**	https://fortiguard.com/advisory/FG-IR-21-200	A-FOR-FORT-201221/141
fortiwlm					
Improper Neutralization of Input	08-Dec-21	3.5	A improper neutralization of input during web page generation ('cross-site	https://fortiguard.com/advisory/FG-	A-FOR-FORT-201221/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			scripting') in Fortinet FortiWLM version 8.6.1 and below allows attacker to store malicious javascript code in the device and trigger it via crafted HTTP requests **CVE ID : CVE-2021-41029**	IR-21-114	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	3.5	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiWLM version 8.6.1 and below allows attacker to execute malicious javascript code on victim's host via crafted HTTP requests **CVE ID : CVE-2021-42752**	https://fortiguard.com/advisory/FG-IR-21-111	A-FOR-FORT-201221/143
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Dec-21	7.5	A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiWLM version 8.6.1 and below allows attacker to disclose sensitive information from DB tables via crafted requests. **CVE ID : CVE-2021-42760**	https://fortiguard.com/advisory/FG-IR-21-129	A-FOR-FORT-201221/144
frentix					
openolat					
Relative Path Traversal	10-Dec-21	7.9	OpenOlat is a web-basedlearning management system. A path traversal vulnerability exists in OpenOlat prior to versions 15.5.12 and 16.0.5. By providing a filename that contains a relative path as a parameter in some REST methods, it is possible to	https://github.com/OpenOLAT/OpenOLAT/commit/336d5ce80681be61a0bbf4f73d2af5d1ff67e93a, https://github.com/Open	A-FRE-OPEN-201221/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			create directory structures and write files anywhere on the target system. The attack could be used to write files anywhere in the web root folder or outside, depending on the configuration of the system and the properly configured permission of the application server user. The attack requires an OpenOlat user account, an enabled REST API and the rights on a business object to call the vulnerable REST calls. The problem is fixed in version 15.5.12 and 16.0.5. There is a workaround available. The vulnerability requires the REST module to be enabled. Disabling the REST module or limiting the REST module via some firewall or web-server access rules to be accessed only be trusted systems will mitigate the risk. **CVE ID : CVE-2021-41242**	OLAT/OpenOLAT/security/advisories/GHSA-62hv-rfp4-hmrm, https://jira.openolat.org/browse/OO-5819	
genesys					
intelligent_workload_distribution_manager					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Dec-21	6.5	A SQL Injection in the custom filter query component in Genesys intelligent Workload Distribution (IWD) before 9.0.013.11 allows an attacker to execute arbitrary SQL queries via the ql_expression parameter, with which all data in the database can be extracted and OS command execution is possible	https://www.offensity.com/en/blog/authenticated-sql-injection-in-the-genesys-iwd-manager-cve-2021-40860-and-	A-GEN-INTE-201221/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			depending on the permissions and/or database engine. **CVE ID : CVE-2021-40860**	cve-2021-40861/, https://docs.genesys.com/Documentation/IWD	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Dec-21	6.5	A SQL Injection in the custom filter query component in Genesys intelligent Workload Distribution (IWD) 9.0.017.07 allows an attacker to execute arbitrary SQL queries via the value attribute, with which all data in the database can be extracted and OS command execution is possible depending on the permissions and/or database engine. **CVE ID : CVE-2021-40861**	https://www.offensity.com/en/blog/authenticated-sql-injection-in-the-genesys-iwd-manager-cve-2021-40860-and-cve-2021-40861/, https://docs.genesys.com/Documentation/IWD	A-GEN-INTE-201221/147
git-it_project					
git-it					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Dec-21	7.5	Git-it through 4.4.0 allows OS command injection at the Branches Aren't Just For Birds challenge step. During the verification process, it attempts to run the reflog command followed by the current branch name (which is not sanitized for execution). **CVE ID : CVE-2021-44685**	N/A	A-GIT-GIT--201221/148
github-todos_project					
github-todos					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Dec-21	7.5	naholyr github-todos 3.1.0 is vulnerable to command injection. The range argument for the _hook subcommand is concatenated without any validation, and is directly used by the exec function. **CVE ID : CVE-2021-44684**	N/A	A-GIT-GITH-201221/149
Gitlab					
gitlab					
Improper Authentication	06-Dec-21	7.5	It was possible to bypass 2FA for LDAP users and access some specific pages with Basic Authentication in GitLab 14.1.1 and above. **CVE ID : CVE-2021-39890**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39890.json	A-GIT-GITL-201221/150
Inadequate Encryption Strength	06-Dec-21	5	Assuming a database breach, nonce reuse issues in GitLab 11.6+ allows an attacker to decrypt some of the database's encrypted content **CVE ID : CVE-2021-22170**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22170.json	A-GIT-GITL-201221/151
globaldatingsoftware					
premiumdatingscript					
Weak Password Recovery Mechanism for Forgotten Password	09-Dec-21	5	An Incorrect Access Control vulnerability exists in Premiumdatingscript 4.2.7.7 via the password change procedure in requests\user.php. **CVE ID : CVE-2021-41694**	N/A	A-GLO-PREM-201221/152
Improper Neutralization of Special Elements	09-Dec-21	7.5	An SQL Injection vulnerability exists in Premiumdatingscript 4.2.7.7 via the ip parameter in	N/A	A-GLO-PREM-201221/153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			connect.php. . **CVE ID : CVE-2021-41695**		
Weak Password Requirements	09-Dec-21	4	An authentication bypass (account takeover) vulnerability exists in Premiumdatingscript 4.2.7.7 due to a weak password reset mechanism in requests\user.php. **CVE ID : CVE-2021-41696**	N/A	A-GLO-PREM-201221/154
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-21	4.3	A reflected Cross Site Scripting (XSS) vulnerability exists in Premiumdatingscript 4.2.7.7 via the aerror_description parameter in assets/sources/instagram.php script. **CVE ID : CVE-2021-41697**	N/A	A-GLO-PREM-201221/155
GNU					
libredwg					
NULL Pointer Dereference	02-Dec-21	5	LibreDWG v0.12.3 was discovered to contain a NULL pointer dereference via out_dxfb.c. **CVE ID : CVE-2021-28236**	N/A	A-GNU-LIBR-201221/156
Out-of-bounds Write	02-Dec-21	7.5	LibreDWG v0.12.3 was discovered to contain a heap-buffer overflow via decode_preR13. **CVE ID : CVE-2021-28237**	N/A	A-GNU-LIBR-201221/157
mailman					
Cross-Site Request	02-Dec-21	6.8	In GNU Mailman before 2.1.38, a list member or	https://bugs.launchpad.ne	A-GNU-MAIL-201221/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			moderator can get a CSRF token and craft an admin request (using that token) to set a new admin password or make other changes. **CVE ID : CVE-2021-44227**	t/mailman/+bug/1952384	
Goautodial					
goautodial					
Improper Authentication	07-Dec-21	5	The GOautodial API prior to commit 3c3a979 made on October 13th, 2021 exposes an API router that accepts a username, password, and action that routes to other PHP files that implement the various API functions. Vulnerable versions of GOautodial validate the username and password incorrectly, allowing the caller to specify any values for these parameters and successfully authenticate. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C **CVE ID : CVE-2021-43175**	N/A	A-GOA-GOAU-201221/159
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Dec-21	6.5	The GOautodial API prior to commit 3c3a979 made on October 13th, 2021 takes a user-supplied “action” parameter and appends a .php file extension to locate and load the correct PHP file to implement the API call. Vulnerable versions of GOautodial do not sanitize the user input that specifies the action. This permits an	N/A	A-GOA-GOAU-201221/160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute any PHP source file with a .php extension that is present on the disk and readable by the GOautodial web server process. Combined with CVE-2021-43175, it is possible for the attacker to do this without valid credentials. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C **CVE ID : CVE-2021-43176**		
goautodial_api					
Improper Authentication	07-Dec-21	5	The GOautodial API prior to commit 3c3a979 made on October 13th, 2021 exposes an API router that accepts a username, password, and action that routes to other PHP files that implement the various API functions. Vulnerable versions of GOautodial validate the username and password incorrectly, allowing the caller to specify any values for these parameters and successfully authenticate. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C **CVE ID : CVE-2021-43175**	N/A	A-GOA-GOAU-201221/161
Improper Limitation of a Pathname to a Restricted Directory	07-Dec-21	6.5	The GOautodial API prior to commit 3c3a979 made on October 13th, 2021 takes a user-supplied “action” parameter and appends a .php file extension to locate	N/A	A-GOA-GOAU-201221/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			and load the correct PHP file to implement the API call. Vulnerable versions of GOautodial do not sanitize the user input that specifies the action. This permits an attacker to execute any PHP source file with a .php extension that is present on the disk and readable by the GOautodial web server process. Combined with CVE-2021-43175, it is possible for the attacker to do this without valid credentials. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C **CVE ID : CVE-2021-43176**		
Google					
exposure_notification_verification_server					
Incorrect Permission Assignment for Critical Resource	09-Dec-21	5.8	An attacker could prematurely expire a verification code, making it unusable by the patient, making the patient unable to upload their TEKs to generate exposure notifications. We recommend upgrading the Exposure Notification server to V1.1.2 or greater. **CVE ID : CVE-2021-22565**	https://github.com/google/exposure-notifications-verification-server/releases/tag/v1.1.2	A-GOO-EXPO-201221/163
grafana					
agent					
Exposure of Sensitive Information to an	08-Dec-21	4.3	Grafana Agent is a telemetry collector for sending metrics, logs, and trace data to the opinionated Grafana	https://github.com/grafana/agent/commit/af7fb0	A-GRA-AGEN-201221/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			observability stack. Prior to versions 0.20.1 and 0.21.2, inline secrets defined within a metrics instance config are exposed in plaintext over two endpoints: metrics instance configs defined in the base YAML file are exposed at `/-/config` and metrics instance configs defined for the scraping service are exposed at `/agent/api/v1/configs/:key`. Inline secrets will be exposed to anyone being able to reach these endpoints. If HTTPS with client authentication is not configured, these endpoints are accessible to unauthenticated users. Secrets found in these sections are used for delivering metrics to a Prometheus Remote Write system, authenticating against a system for discovering Prometheus targets, and authenticating against a system for collecting metrics. This does not apply for non-inlined secrets, such as `*_file` based secrets. This issue is patched in Grafana Agent versions 0.20.1 and 0.21.2. A few workarounds are available. Users who cannot upgrade should use non-inline secrets where possible. Users may also desire to restrict API access to Grafana Agent with	1e31fe2d389e5f1c36b399ddc46b412b21, https://github.com/grafana/agent/pull/1152, https://github.com/grafana/agent/security/advisories/GHSA-9c4x-5hgq-q3wh	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some combination of restricting the network interfaces Grafana Agent listens on through `http_listen_address` in the `server` block, configuring Grafana Agent to use HTTPS with client authentication, and/or using firewall rules to restrict external access to Grafana Agent's API. **CVE ID : CVE-2021-41090**		
grafana					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Dec-21	5	Grafana is an open-source platform for monitoring and observability. Grafana versions 8.0.0-beta1 through 8.3.0 (except for patched versions) iss vulnerable to directory traversal, allowing access to local files. The vulnerable URL path is: `<grafana_host_url>/public/plugins//`, where is the plugin ID for any installed plugin. At no time has Grafana Cloud been vulnerable. Users are advised to upgrade to patched versions 8.0.7, 8.1.8, 8.2.7, or 8.3.1. The GitHub Security Advisory contains more information about vulnerable URL paths, mitigation, and the disclosure timeline. **CVE ID : CVE-2021-43798**	https://github.com/grafana/grafana/security/advisories/GHSA-8pjx-jj86-j47p, https://github.com/grafana/grafana/commit/c798c0e958d15d9cc7f27c72113d572fa58545ce, http://www.openwall.com/lists/oss-security/2021/12/09/2	A-GRA-GRAF-201221/165
Improper Limitation of a Pathname	10-Dec-21	4	Grafana is an open-source platform for monitoring and observability. Grafana prior	https://github.com/grafana/grafana/c	A-GRA-GRAF-201221/166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			to versions 8.3.2 and 7.5.12 contains a directory traversal vulnerability for fully lowercase or fully uppercase .md files. The vulnerability is limited in scope, and only allows access to files with the extension .md to authenticated users only. Grafana Cloud instances have not been affected by the vulnerability. Users should upgrade to patched versions 8.3.2 or 7.5.12. For users who cannot upgrade, running a reverse proxy in front of Grafana that normalizes the PATH of the request will mitigate the vulnerability. The proxy will have to also be able to handle url encoded paths. Alternatively, for fully lowercase or fully uppercase .md files, users can block /api/plugins/.*/markdown/.* without losing any functionality beyond inlined plugin help text. **CVE ID : CVE-2021-43813**	ommit/fd48aee61e4328aae8d5303a9efd045fa0ca308d, https://grafana.com/blog/2021/12/10/grafana-8.3.2-and-7.5.12-released-with-moderate-severity-security-fix/, http://www.openwall.com/lists/oss-security/2021/12/10/4	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Dec-21	3.5	Grafana is an open-source platform for monitoring and observability. Grafana prior to versions 8.3.2 and 7.5.12 has a directory traversal for arbitrary .csv files. It only affects instances that have the developer testing tool called TestData DB data source enabled and configured. The vulnerability	https://github.com/grafana/grafana/security/advisories/GHSA-7533-c8qv-jm9m, https://github.com/grafana/grafana/commit/fd48a	A-GRA-GRAF-201221/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is limited in scope, and only allows access to files with the extension .csv to authenticated users only. Grafana Cloud instances have not been affected by the vulnerability. Versions 8.3.2 and 7.5.12 contain a patch for this issue. There is a workaround available for users who cannot upgrade. Running a reverse proxy in front of Grafana that normalizes the PATH of the request will mitigate the vulnerability. The proxy will have to also be able to handle url encoded paths. **CVE ID : CVE-2021-43815**	ee61e4328aae8d5303a9efd045fa0ca308d, https://github.com/grafana/grafana/commit/d6ec6f8ad28f0212e584406730f939105ff6c6d3	
h2database					
h2					
Improper Restriction of XML External Entity Reference	10-Dec-21	6.4	The package com.h2database:h2 from 0 and before 2.0.202 are vulnerable to XML External Entity (XXE) Injection via the org.h2.jdbc.JdbcSQLXML class object, when it receives parsed string data from org.h2.jdbc.JdbcResultSet.getSQLXML() method. If it executes the getSource() method when the parameter is DOMSource.class it will trigger the vulnerability. **CVE ID : CVE-2021-23463**	https://github.com/h2database/h2database/issues/3195, https://snyk.io/vuln/SNYK-JAVA-COMH2DATABASE-1769238, https://github.com/h2database/h2database/pull/3199	A-H2D-H2-201221/168
haschek					
pictshare					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-21	4.3	pictshare v1.5 is affected by a Cross Site Scripting (XSS) vulnerability in api/info.php. The exit function will terminate the script and print the message which has $_REQUEST['hash']. **CVE ID : CVE-2021-43683**	N/A	A-HAS-PICT-201221/169
hashicorp					
consul					
Incorrect Authorization	12-Dec-21	6.5	HashiCorp Consul Enterprise before 1.8.17, 1.9.x before 1.9.11, and 1.10.x before 1.10.4 has Incorrect Access Control. An ACL token (with the default operator:write permissions) in one namespace can be used for unintended privilege escalation in a different namespace. **CVE ID : CVE-2021-41805**	https://www.hashicorp.com/blog/category/consul, https://discuss.hashicorp.com/t/hcsec-2021-29-consul-enterprise-namespace-default-acls-allow-privilege-escalation/31871	A-HAS-CONS-201221/170
nomad					
Improper Authentication	03-Dec-21	6	HashiCorp Nomad and Nomad Enterprise up to 1.0.13, 1.1.7, and 1.2.0, with the QEMU task driver enabled, allowed authenticated users with job submission capabilities to bypass the configured allowed image paths. Fixed in 1.0.14, 1.1.8, and 1.2.1.	https://discuss.hashicorp.com/t/hcsec-2021-31-nomad-qemu-task-driver-allowed-paths-bypass-with-job-	A-HAS-NOMA-201221/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-43415	args/32288, https://www.hashicorp.com/blog/category/nomad	
HP					
storeserv_management_console					
Improper Control of Generation of Code ('Code Injection')	10-Dec-21	6.5	A security vulnerability has been identified in HPE StoreServ Management Console (SSMC). An authenticated SSMC administrator could exploit the vulnerability to inject code and elevate their privilege in SSMC. The scope of this vulnerability is limited to SSMC. Note: The arrays being managed are not impacted by this vulnerability. This vulnerability impacts SSMC versions 3.4 GA to 3.8.1. **CVE ID : CVE-2021-29214**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04207en_us	A-HP-STOR-201221/172
huntflow					
huntflow_enterprise					
Improper Restriction of Excessive Authentication Attempts	10-Dec-21	5	Due to insufficient server-side login-attempt limit enforcement, a vulnerability in /account/login in Huntflow Enterprise before 3.10.14 could allow an unauthenticated, remote user to perform multiple login attempts for brute-force password guessing. **CVE ID : CVE-2021-37934**	N/A	A-HUN-HUNT-201221/173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	10-Dec-21	5	An information disclosure vulnerability in the login page of Huntflow Enterprise before 3.10.4 could allow an unauthenticated, remote user to get information about the domain name of the configured LDAP server. An attacker could exploit this vulnerability by requesting the login page and searching for the "isLdap" JavaScript parameter in the HTML source code. **CVE ID : CVE-2021-37935**	N/A	A-HUN-HUNT-201221/174
IBM					
cognos_analytics					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Dec-21	3.5	IBM Cognos Analytics 11.1.7 and 11.2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 209706. **CVE ID : CVE-2021-38909**	https://www.ibm.com/support/pages/node/6520510, https://exchange.xforce.ibmcloud.com/vulnerabilities/209706	A-IBM-COGN-201221/175
Weak Password Requirements	03-Dec-21	5	IBM Cognos Analytics 11.1.7 and 11.2.0 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 196339. **CVE ID : CVE-2021-20470**	https://exchange.xforce.ibmcloud.com/vulnerabilities/196939, https://www.ibm.com/support/pages/node/6520	A-IBM-COGN-201221/176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				510	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Dec-21	4.3	IBM Cognos Analytics 11.1.7 and 11.2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 197794. **CVE ID : CVE-2021-20493**	https://www.ibm.com/support/pages/node/6520510	A-IBM-COGN-201221/177
Exposure of Resource to Wrong Sphere	03-Dec-21	4	IBM Cognos Analytics 11.1.7 and 11.2.0 could allow a low level user to reas of the application that privileged user should only be allowed to view. IBM X-Force ID: 201087. **CVE ID : CVE-2021-29716**	https://www.ibm.com/support/pages/node/6520510, https://exchange.xforce.ibmcloud.com/vulnerabilities/201087	A-IBM-COGN-201221/178
Exposure of Resource to Wrong Sphere	03-Dec-21	5	IBM Cognos Analytics 11.1.7 and 11.2.0 could be vulnerable to client side vulnerabilties due to a web response specifying an incorrect content type. IBM X-Force ID: 201091 **CVE ID : CVE-2021-29719**	https://www.ibm.com/support/pages/node/6520510, https://exchange.xforce.ibmcloud.com/vulnerabilities/201091	A-IBM-COGN-201221/179
Cross-Site Request Forgery (CSRF)	03-Dec-21	6.8	IBM Cognos Analytics 11.1.7 and 11.2.0 is vulnerable to cross-site request forgery (CSRF) in the My Inbox page which could allow an attacker	https://www.ibm.com/support/pages/node/6520510,	A-IBM-COGN-201221/180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 202167. **CVE ID : CVE-2021-29756**	https://exchange.xforce.ibmcloud.com/vulnerabilities/202167	
Exposure of Resource to Wrong Sphere	03-Dec-21	5.5	IBM Cognos Analytics 11.1.7 and 11.2.0 could allow an authenticated to view or edit a Jupyter notebook that they should not have access to. IBM X-Force ID: 206212. **CVE ID : CVE-2021-29867**	https://www.ibm.com/support/pages/node/6520510, https://exchange.xforce.ibmcloud.com/vulnerabilities/206212	A-IBM-COGN-201221/181
db2					
Improper Privilege Management	09-Dec-21	2.1	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to gain privileges due to allowing modification of columns of existing tasks. IBM X-Force ID: 210321. **CVE ID : CVE-2021-38926**	https://exchange.xforce.ibmcloud.com/vulnerabilities/210321, https://www.ibm.com/support/pages/node/6523808	A-IBM-DB2-201221/182
Exposure of Resource to Wrong Sphere	09-Dec-21	4	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1, and 11.5 is vulnerable to an information disclosure as a result of a connected user having indirect read access to a table where they are not authorized to select from. IBM X-Force ID: 210418. **CVE ID : CVE-2021-38931**	https://www.ibm.com/support/pages/node/6523810, https://exchange.xforce.ibmcloud.com/vulnerabilities/210418	A-IBM-DB2-201221/183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of a Broken or Risky Cryptographic Algorithm	09-Dec-21	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID : CVE-2021-39002**	https://exchange.xforce.ibmcloud.com/vulnerabilities/213217, https://www.ibm.com/support/pages/node/6523802	A-IBM-DB2-201221/184
Exposure of Resource to Wrong Sphere	09-Dec-21	5	IBM Db2 9.7, 10.1, 10.5, 11.1, and 11.5 may be vulnerable to an Information Disclosure when using the LOAD utility as under certain circumstances the LOAD utility does not enforce directory restrictions. IBM X-Force ID: 199521. **CVE ID : CVE-2021-20373**	https://www.ibm.com/support/pages/node/6523804, https://exchange.xforce.ibmcloud.com/vulnerabilities/195521	A-IBM-DB2-201221/185
Incorrect Authorization	09-Dec-21	5.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a user with DBADM authority to access other databases and read or modify files. IBM X-Force ID: 199914. **CVE ID : CVE-2021-29678**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199914, https://www.ibm.com/support/pages/node/6523806	A-IBM-DB2-201221/186
qradar_security_information_and_event_manager					
Inadequate Encryption Strength	01-Dec-21	5	IBM QRadar SIEM 7.3 and 7.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 196074. **CVE ID : CVE-2021-20400**	https://exchange.xforce.ibmcloud.com/vulnerabilities/196074, https://www.ibm.com/support/page	A-IBM-QRAD-201221/187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				s/node/6520488	
Improper Authentication	01-Dec-21	4.3	IBM QRadar SIEM 7.3 and 7.4 could allow an attacker to obtain sensitive information due to the server performing key exchange without entity authentication on inter-host communications using man in the middle techniques. IBM X-Force ID: 203033. **CVE ID : CVE-2021-29779**	https://www.ibm.com/support/pages/node/6520484, https://exchange.xforce.ibmcloud.com/vulnerabilities/203033	A-IBM-QRAD-201221/188
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	4.3	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 205281. **CVE ID : CVE-2021-29849**	https://www.ibm.com/support/pages/node/6520476, https://exchange.xforce.ibmcloud.com/vulnerabilities/205281	A-IBM-QRAD-201221/189
Server-Side Request Forgery (SSRF)	01-Dec-21	4	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to server side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. This vulnerability is due to an incomplete fix for CVE-2020-4786. IBM X-Force ID: 206087. **CVE ID : CVE-2021-29863**	https://exchange.xforce.ibmcloud.com/vulnerabilities/206087, https://www.ibm.com/support/pages/node/6520490	A-IBM-QRAD-201221/190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
websphere_application_server					
Uncontrolled Resource Consumption	09-Dec-21	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available CPU resources. IBM X-Force ID: 211405. **CVE ID : CVE-2021-38951**	https://www.ibm.com/support/pages/node/6524674, https://exchange.xforce.ibmcloud.com/vulnerabilities/211405	A-IBM-WEBS-201221/191
inveniosoftware					
invenio-drafts-resources					
Missing Authorization	06-Dec-21	4	Invenio-Drafts-Resources is a submission/deposit module for Invenio, a software framework for research data management. Invenio-Drafts-Resources prior to versions 0.13.7 and 0.14.6 does not properly check permissions when a record is published. The vulnerability is exploitable in a default installation of InvenioRDM. An authenticated a user is able via REST API calls to publish draft records of other users if they know the record identifier and the draft validates (e.g. all require fields filled out). An attacker is not able to modify the data in the record, and thus e.g. *cannot* change a record from restricted to public. The problem is patched in Invenio-Drafts-Resources	https://github.com/inveniosoftware/invenio-drafts-resources/commit/039b0cff1ad4b952000f4d8c3a93f347108b6626, https://github.com/inveniosoftware/invenio-drafts-resources/security/advisories/GHSA-xr38-w74q-r8jv	A-INV-INVE-201221/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v0.13.7 and 0.14.6, which is part of InvenioRDM v6.0.1 and InvenioRDM v7.0 respectively. **CVE ID : CVE-2021-43781**		
ivanti					
avalanche					
Incorrect Authorization	07-Dec-21	6.5	An improper access control vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to perform a session takeover. **CVE ID : CVE-2021-42124**	https://forums.ivanti.com/s/article/Security-Alert-CVE-s-Addressed-in-Avalanche-6-3-3	A-IVA-AVAL-201221/193
Unrestricted Upload of File with Dangerous Type	07-Dec-21	6.5	An unrestricted file upload vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to write dangerous files. **CVE ID : CVE-2021-42125**	https://forums.ivanti.com/s/article/Security-Alert-CVE-s-Addressed-in-Avalanche-6-3-3	A-IVA-AVAL-201221/194
Incorrect Authorization	07-Dec-21	6.5	An improper authorization control vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to perform privilege escalation. **CVE ID : CVE-2021-42126**	https://forums.ivanti.com/s/article/Security-Alert-CVE-s-Addressed-in-Avalanche-6-3-3	A-IVA-AVAL-201221/195
Deserialization of Untrusted Data	07-Dec-21	7.5	A deserialization of untrusted data vulnerability exists in Ivanti Avalanche before 6.3.3 using Inforail Service allows arbitrary code execution via	https://forums.ivanti.com/s/article/Security-Alert-CVE-s-	A-IVA-AVAL-201221/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Data Repository Service. **CVE ID : CVE-2021-42127**	Addressed-in-Avalanche-6-3-3	
Improper Privilege Management	07-Dec-21	7.5	An exposed dangerous function vulnerability exists in Ivanti Avalanche before 6.3.3 using inforail Service allows Privilege Escalation via Enterprise Server Service. **CVE ID : CVE-2021-42128**	https://forums.ivanti.com/s/article/Security-Alert-CVE-s-Addressed-in-Avalanche-6-3-3	A-IVA-AVAL-201221/197
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-21	6.5	A command injection vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to perform arbitrary command execution. **CVE ID : CVE-2021-42129**	https://forums.ivanti.com/s/article/Security-Alert-CVE-s-Addressed-in-Avalanche-6-3-3	A-IVA-AVAL-201221/198
Deserialization of Untrusted Data	07-Dec-21	6.5	A deserialization of untrusted data vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to perform arbitrary code execution. **CVE ID : CVE-2021-42130**	https://forums.ivanti.com/s/article/Security-Alert-CVE-s-Addressed-in-Avalanche-6-3-3	A-IVA-AVAL-201221/199
Improper Neutralization of Special Elements used in an SQL Command ('SQL	07-Dec-21	6.5	A SQL Injection vulnerability exists in Ivanti Avalance before 6.3.3 allows an attacker with access to the Inforail Service to perform privilege escalation. **CVE ID : CVE-2021-42131**	https://forums.ivanti.com/s/article/Security-Alert-CVE-s-Addressed-in-Avalanche-6-	A-IVA-AVAL-201221/200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')				3-3	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-21	6.5	A command Injection vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to perform arbitrary command execution. **CVE ID : CVE-2021-42132**	https://forums.ivanti.com/s/article/Security-Alert-CVE-s-Addressed-in-Avalanche-6-3-3	A-IVA-AVAL-201221/201
Inclusion of Functionality from Untrusted Control Sphere	07-Dec-21	5.5	An exposed dangerous function vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to perform an arbitrary file write. **CVE ID : CVE-2021-42133**	https://forums.ivanti.com/s/article/Security-Alert-CVE-s-Addressed-in-Avalanche-6-3-3	A-IVA-AVAL-201221/202
endpoint_manager_cloud_services_appliance					
Improper Control of Generation of Code ('Code Injection')	08-Dec-21	7.5	A code injection vulnerability in the Ivanti EPM Cloud Services Appliance (CSA) allows an unauthenticated user to execute arbitrary code with limited permissions (nobody). **CVE ID : CVE-2021-44529**	https://forums.ivanti.com/s/article/SA-2021-12-02	A-IVA-ENDP-201221/203
Jamf					
jamf					
Server-Side Request Forgery (SSRF)	01-Dec-21	6.5	An issue was discovered in Jamf Pro before 10.32.0, aka PI-009921. An account can be granted incorrect privileges in response to authentication that uses specific sign-on workflows. **CVE ID : CVE-2021-40809**	https://www.jamf.com/resources/product-documentation/jamf-pro-release-notes/,	A-JAM-JAMF-201221/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://docs.jamf.com/10.32.0/jamf-pro/release-notes/Resolved_Issues.html	
Johnsoncontrols					
kantech_entrapass					
Exposure of Resource to Wrong Sphere	06-Dec-21	5	Successful exploitation of this vulnerability could allow an unauthorized user to access sensitive data. **CVE ID : CVE-2021-36198**	https://www.johnsoncontrols.com/cyber-solutions/security-advisories	A-JOH-KANT-201221/205
julialang					
julia					
Out-of-bounds Read	08-Dec-21	6.4	An out-of-bounds read flaw was found in the CLARRV, DLARRV, SLARRV, and ZLARRV functions in lapack through version 3.10.0, as also used in OpenBLAS before version 0.3.18. Specially crafted inputs passed to these functions could cause an application using lapack to crash or possibly disclose portions of its memory. **CVE ID : CVE-2021-4048**	https://github.com/JuliaLang/julia/issues/42415, https://github.com/xianyi/OpenBLAS/commit/337b65133df174796794871b3988cd03426e6d41, https://github.com/xianyi/OpenBLAS/commit/2be5ee3cca97a597f2ee2118808a2d5eacea050c	A-JUL-JULI-201221/206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Kaseya					
unitrends_backup					
Improper Input Validation	06-Dec-21	10	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. Multiple functions in the bpserverd daemon were vulnerable to arbitrary remote code execution as root. The vulnerability was caused by untrusted input (received by the server) being passed to system calls. **CVE ID : CVE-2021-43033**	https://helpdesk.kaseya.com/hc/en-gb/articles/4412762258961	A-KAS-UNIT-201221/207
Improper Privilege Management	06-Dec-21	4.6	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. A world writable file allowed local users to execute arbitrary code as the user apache, leading to privilege escalation. **CVE ID : CVE-2021-43034**	https://helpdesk.kaseya.com/hc/en-gb/articles/4412762258961	A-KAS-UNIT-201221/208
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Dec-21	7.5	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. Two unauthenticated SQL injection vulnerabilities were discovered, allowing arbitrary SQL queries to be injected and executed under the postgres superuser account. Remote code execution was possible, leading to full access to the postgres user account. **CVE ID : CVE-2021-43035**	https://helpdesk.kaseya.com/hc/en-gb/articles/4412762258961	A-KAS-UNIT-201221/209
Weak	06-Dec-21	7.5	An issue was discovered in	https://help	A-KAS-UNIT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Password Requirements			Kaseya Unitrends Backup Appliance before 10.5.5. The password for the PostgreSQL wguest account is weak. **CVE ID : CVE-2021-43036**	desk.kaseya.com/hc/en-gb/articles/44127622589 61	201221/210
Uncontrolled Search Path Element	06-Dec-21	6.9	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. The Unitrends Windows agent was vulnerable to DLL injection and binary planting due to insecure default permissions. This allowed privilege escalation from an unprivileged user to SYSTEM. **CVE ID : CVE-2021-43037**	https://helpdesk.kaseya.com/hc/en-gb/articles/44127622589 61	A-KAS-UNIT-201221/211
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Dec-21	6.5	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. The wguest account could execute commands by injecting into PostgreSQL trigger functions. This allowed privilege escalation from the wguest user to the postgres user. **CVE ID : CVE-2021-43038**	https://helpdesk.kaseya.com/hc/en-gb/articles/44127622589 61	A-KAS-UNIT-201221/212
Exposure of Resource to Wrong Sphere	06-Dec-21	6.4	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. The Samba file sharing service allowed anonymous read/write access. **CVE ID : CVE-2021-43039**	https://helpdesk.kaseya.com/hc/en-gb/articles/44127622589 61	A-KAS-UNIT-201221/213
Improper Privilege Management	06-Dec-21	6.5	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. The privileged vaultServer could be leveraged to create arbitrary writable files,	https://helpdesk.kaseya.com/hc/en-gb/articles/44127622589	A-KAS-UNIT-201221/214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to privilege escalation. **CVE ID : CVE-2021-43040**	61	
Use of Externally-Controlled Format String	06-Dec-21	6.5	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. A crafted HTTP request could induce a format string vulnerability in the privileged vaultServer application. **CVE ID : CVE-2021-43041**	https://helpdesk.kaseya.com/hc/en-gb/articles/44127622589 61	A-KAS-UNIT-201221/215
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-21	7.5	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. A buffer overflow existed in the vaultServer component. This was exploitable by a remote unauthenticated attacker. **CVE ID : CVE-2021-43042**	https://helpdesk.kaseya.com/hc/en-gb/articles/44127622589 61	A-KAS-UNIT-201221/216
Exposure of Resource to Wrong Sphere	06-Dec-21	4	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. The apache user could read arbitrary files such as /etc/shadow by abusing an insecure Sudo rule. **CVE ID : CVE-2021-43043**	https://helpdesk.kaseya.com/hc/en-gb/articles/44127622589 61	A-KAS-UNIT-201221/217
Use of Hard-coded Credentials	06-Dec-21	7.5	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. The SNMP daemon was configured with a weak default community. **CVE ID : CVE-2021-43044**	https://helpdesk.kaseya.com/hc/en-gb/articles/44127622589 61	A-KAS-UNIT-201221/218
kb					
digger					
Improper	08-Dec-21	6.4	National Library of the	https://githu	A-KB-DIGG-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of XML External Entity Reference			Netherlands digger < 6697d1269d981e35e11f240725b16401b5ce3db5 is affected by a XML External Entity (XXE) vulnerability. Since XML parsing resolves external entities, a malicious XML stream could leak internal files and/or cause a DoS. **CVE ID : CVE-2021-44556**	b.com/KBNLresearch/digger/pull/1	201221/219
multiner					
Improper Restriction of XML External Entity Reference	08-Dec-21	6.4	National Library of the Netherlands multiNER <= c0440948057afc6e3d6b4903a7c05e666b94a3bc is affected by an XML External Entity (XXE) vulnerability in multiNER/ner.py. Since XML parsing resolves external entities, a malicious XML stream could leak internal files and/or cause a DoS. **CVE ID : CVE-2021-44557**	https://github.com/KBNLresearch/multiNER/pull/3	A-KB-MULT-201221/220
Kentico					
xperience					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Dec-21	3.5	The Kentico Xperience CMS version 13.0 – 13.0.43 is vulnerable to a persistent Cross-Site Scripting (XSS) vulnerability (also known as Stored or Second-Order XSS). Persistent XSS vulnerabilities occur when the application stores and retrieves client supplied data without proper handling of dangerous content. This type of XSS vulnerability is exploited by	N/A	A-KEN-XPER-201221/221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			submitting malicious script content to the application which is then retrieved and executed by other application users. The attacker could exploit this to conduct a range of attacks against users of the affected application such as session hijacking, account take over and accessing sensitive data. **CVE ID : CVE-2021-43991**		
kimai					
kimai2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	6	kimai2 is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-3985**	https://github.com/kevinpapst/kimai2/commit/76e09447c85e762882126b49626a4fe4d93fe8b5, https://huntr.dev/bounties/89d6c3de-efbd-4354-8cc8-46e999e4c5a4	A-KIM-KIMA-201221/222
kimai_2					
Cross-Site Request Forgery (CSRF)	09-Dec-21	4.3	kimai2 is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-4033**	https://github.com/kevinpapst/kimai2/commit/1da26e041df62c10bd8075d78f2db7854d3eee07, https://hunt	A-KIM-KIMA-201221/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				r.dev/bounties/e05be1f7-d00c-4cfd-9390-ccd9d1c737b7	
kimai2_project					
kimai2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	4.3	kimai2 is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-3983**	https://github.com/kevinpapst/kimai2/commit/89bfa82c61da0d3639e4038e689e25467baac8a0, https://huntr.dev/bounties/c96f3480-dccf-4cc2-99a4-d2b3a7462413	A-KIM-KIMA-201221/224
Incorrect Authorization	01-Dec-21	4	kimai2 is vulnerable to Improper Access Control **CVE ID : CVE-2021-3992**	https://huntr.dev/bounties/a0c438fb-c8e1-40cf-acc6-c8a532b80b93, https://github.com/kevinpapst/kimai2/commit/ff9acab0fc81f0e9490462739ef15fe4ab028ea5	A-KIM-KIMA-201221/225
knime					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
knime_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-21	5	KNIME Server before 4.13.4 allows directory traversal in a request for a client profile. **CVE ID : CVE-2021-44725**	https://docs.knime.com/2021-06/server_update_guide/index.html#_bugfixes	A-KNI-KNIM-201221/226
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	KNIME Server before 4.13.4 allows XSS via the old WebPortal login page. **CVE ID : CVE-2021-44726**	https://docs.knime.com/2021-06/server_update_guide/index.html#_bugfixes	A-KNI-KNIM-201221/227
lapack_project					
lapack					
Out-of-bounds Read	08-Dec-21	6.4	An out-of-bounds read flaw was found in the CLARRV, DLARRV, SLARRV, and ZLARRV functions in lapack through version 3.10.0, as also used in OpenBLAS before version 0.3.18. Specially crafted inputs passed to these functions could cause an application using lapack to crash or possibly disclose portions of its memory. **CVE ID : CVE-2021-4048**	https://github.com/JuliaLang/julia/issues/42415, https://github.com/xianyi/OpenBLAS/commit/337b65133df174796794871b3988cd03426e6d41, https://github.com/xianyi/OpenBLAS/commit/2be5ee3cca97a597f2ee2118808a2d5eacea050c	A-LAP-LAPA-201221/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Laravel					
framework					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	Laravel is a web application framework. Laravel prior to versions 8.75.0, 7.30.6, and 6.20.42 contain a possible cross-site scripting (XSS) vulnerability in the Blade templating engine. A broken HTML element may be clicked and the user taken to another location in their browser due to XSS. This is due to the user being able to guess the parent placeholder SHA-1 hash by trying common names of sections. If the parent template contains an exploitable HTML structure an XSS vulnerability can be exposed. This vulnerability has been patched in versions 8.75.0, 7.30.6, and 6.20.42 by determining the parent placeholder at runtime and using a random hash that is unique to each request. **CVE ID : CVE-2021-43808**	https://github.com/laravel/framework/commit/b8174169b1807f36de1837751599e2828ceddb9b, https://github.com/laravel/framework/pull/39909, https://github.com/laravel/framework/pull/39908, https://github.com/laravel/framework/pull/39906	A-LAR-FRAM-201221/229
laravel					
Deserialization of Untrusted Data	06-Dec-21	7.5	Laravel v5.1 was discovered to contain a deserialization vulnerability via the component \Mockery\Generator\DefinedTargetClass. **CVE ID : CVE-2021-37298**	N/A	A-LAR-LARA-201221/230
librenms					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
librenms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	4.3	Librenms 21.11.0 is affected by a Cross Site Scripting (XSS) vulnerability in includes/html/common/alert-log.inc.php. **CVE ID : CVE-2021-44277**	https://github.com/librenms/librenms/pull/13554	A-LIB-LIBR-201221/231
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Dec-21	7.5	Librenms 21.11.0 is affected by a path manipulation vulnerability in includes/html/pages/device/showconfig.inc.php. **CVE ID : CVE-2021-44278**	https://github.com/librenms/librenms/pull/13554	A-LIB-LIBR-201221/232
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	4.3	Librenms 21.11.0 is affected by a Cross Site Scripting (XSS) vulnerability in includes/html/forms/poller-groups.inc.php. **CVE ID : CVE-2021-44279**	https://github.com/librenms/librenms/pull/13554	A-LIB-LIBR-201221/233
libretime					
libretime_hv					
Externally Controlled Reference to a Resource in Another Sphere	01-Dec-21	7.5	libretime hv3.0.0-alpha.10 is affected by a path manipulation vulnerability in /blob/master/legacy/application/modules/rest/controllers/ShowImageController.php through the rename function. **CVE ID : CVE-2021-43685**	N/A	A-LIB-LIBR-201221/234
Linecorp					
armeria					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Dec-21	5	Armeria is an open source microservice framework. In affected versions an attacker can access an Armeria server's local file system beyond its restricted directory by sending an HTTP request whose path contains `%2F` (encoded `/`), such as `/files/..%2Fsecrets.txt`, bypassing Armeria's path validation logic. Armeria 1.13.4 or above contains the hardened path validation logic that handles `%2F` properly. This vulnerability can be worked around by inserting a decorator that performs an additional validation on the request path. **CVE ID : CVE-2021-43795**	https://github.com/line/armeria/commit/e2697a575e9df6692b423e02d731f293c1313284, https://github.com/line/armeria/security/advisories/GHSA-8fp4-rp6c-5gcv	A-LIN-ARME-201221/235
Linuxfoundation					
runc					
Integer Overflow or Wraparound	06-Dec-21	6	runc is a CLI tool for spawning and running containers on Linux according to the OCI specification. In runc, netlink is used internally as a serialization system for specifying the relevant container configuration to the `C` portion of the code (responsible for the based namespace setup of containers). In all versions of runc prior to 1.0.3, the encoder did not handle the possibility of an integer	https://github.com/opencontainers/runc/commit/d72d057ba794164c3cce9451a00b72a78b25e1ae, https://github.com/opencontainers/runc/commit/9c444070ec7bb83995dbc0185da68284da71c554,	A-LIN-RUNC-201221/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow in the 16-bit length field for the byte array attribute type, meaning that a large enough malicious byte array attribute could result in the length overflowing and the attribute contents being parsed as netlink messages for container configuration. This vulnerability requires the attacker to have some control over the configuration of the container and would allow the attacker to bypass the namespace restrictions of the container by simply adding their own netlink payload which disables all namespaces. The main users impacted are those who allow untrusted images with untrusted configurations to run on their machines (such as with shared cloud infrastructure). runc version 1.0.3 contains a fix for this bug. As a workaround, one may try disallowing untrusted namespace paths from your container. It should be noted that untrusted namespace paths would allow the attacker to disable namespace protections entirely even in the absence of this bug. **CVE ID : CVE-2021-43784**	https://github.com/opencontainers/runc/security/advisories/GHSA-v95c-p5hm-xq8f	
livehelperchat					
live_helper_chat					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	07-Dec-21	4.3	livehelperchat is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-4049**	https://github.com/livehelperchat/livehelperchat/commit/e7fe1aa6a087d4d21b2e8a0dadd2e08f42acbb57, https://huntr.dev/bounties/62408fa4-2c16-4fcd-8b34-41fcdccb779e	A-LIV-LIVE-201221/237
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-4050**	https://github.com/livehelperchat/livehelperchat/commit/0ce1dd2a13509747c240c8484228a5df8d6e03ec, https://huntr.dev/bounties/27eb39d7-7636-4c4b-922c-a2f8fbe1ba05	A-LIV-LIVE-201221/238
m-files					
m-files_web					
Inconsistent Interpretation of HTTP Requests ('HTTP Request	05-Dec-21	7.8	** DISPUTED ** M-Files Web before 20.10.9524.1 allows a denial of service via overlapping ranges (in HTTP requests with crafted Range or Request-Range headers).	https://www.m-files.com/company/trust-center/vulne	A-M-F-M-FI-201221/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Smuggling')			NOTE: this is disputed because the range behavior is the responsibility of the web server, not the responsibility of the individual web application. **CVE ID : CVE-2021-37253**	rability-disclosure/	
mahadiscom					
mahavitaran					
Improper Authenticati on	07-Dec-21	7.5	Maharashtra State Electricity Board Mahavitara Android Application 8.20 and prior is vulnerable to remote account takeover due to OTP fixation vulnerability in password rest function **CVE ID : CVE-2021-41716**	N/A	A-MAH-MAHA-201221/240
manage_project					
manage					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	4.3	manage (last update Oct 24, 2017) is affected by a Cross Site Scripting (XSS) vulnerability in Application/Home/Controlle r/GoodsController.class.php. The exit function will terminate the script and print a message which have values from $_POST. **CVE ID : CVE-2021-43689**	N/A	A-MAN-MANA-201221/241
markdown_to_pdf_project					
markdown_to_pdf					
N/A	10-Dec-21	7.5	The package md-to-pdf before 5.0.0 are vulnerable to Remote Code Execution (RCE) due to utilizing the library gray-matter to parse	https://githu b.com/simon haenisch/md -to-pdf/commit/	A-MAR-MARK-201221/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			front matter content, without disabling the JS engine. **CVE ID : CVE-2021-23639**	a716259c548c82fa1d3b14a3422e9100619d2d8a, https://snyk.io/vuln/SNYK-JS-MDTOPDF-1657880, https://github.com/simonhaenisch/md-to-pdf/issues/99	
mattermost					
mattermost					
Insertion of Sensitive Information into Log File	09-Dec-21	5	Mattermost 6.0.2 and earlier fails to sufficiently sanitize user's password in audit logs when user creation fails. **CVE ID : CVE-2021-37861**	https://mattermost.com/security-updates/	A-MAT-MATT-201221/243
max-3000					
maxsite_cms					
N/A	10-Dec-21	7.5	Remote Code Execution (RCE) vulnerability exists in MaxSite CMS v107.5 via the Documents page. **CVE ID : CVE-2021-27983**	N/A	A-MAX-MAXS-201221/244
Mcafee					
database_security					
Files or Directories Accessible to External Parties	08-Dec-21	5.5	A denial-of-service vulnerability in Database Security (DBS) prior to 4.8.4 allows a remote authenticated administrator to trigger a denial-of-service	https://kc.mcafee.com/corporate/index?page=content&id=SB10358	A-MCA-DATA-201221/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack against the DBS server. The configuration of Archiving through the User interface incorrectly allowed the creation of directories and files in Windows system directories and other locations where sensitive data could be overwritten. The former could lead to a DoS, whilst the latter could lead to data destruction on the DBS server. **CVE ID : CVE-2021-31850**		
network_security_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-21	3.5	Cross Site Scripting (XSS) vulnerability in McAfee Network Security Manager (NSM) prior to 10.1 Minor 7 allows a remote authenticated administrator to embed a XSS in the administrator interface via specially crafted custom rules containing HTML. NSM did not correctly sanitize custom rule content in all scenarios. **CVE ID : CVE-2021-4038**	https://kc.mcafee.com/corporate/index?page=content&id=SB10375	A-MCA-NETW-201221/246
merge-deep2_project					
merge-deep2					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	10-Dec-21	7.5	All versions of package merge-deep2 are vulnerable to Prototype Pollution via the mergeDeep() function. **CVE ID : CVE-2021-23700**	https://snyk.io/vuln/SNYK-JS-MERGEDEEP2-1727593	A-MER-MERG-201221/247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Mozilla					
firefox					
Incorrect Authorization	08-Dec-21	7.5	The iframe sandbox rules were not correctly applied to XSLT stylesheets, allowing an iframe to bypass restrictions such as executing scripts or navigating the top-level frame. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38503**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://bugzilla.mozilla.org/show_bug.cgi?id=1729517, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/	A-MOZ-FIRE-201221/248
Use After Free	08-Dec-21	7.5	When interacting with an HTML input element's file picker dialog with webkitdirectory set, a use-after-free could have resulted, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38504**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://bugzilla.mozilla.org/show_bug.cgi?id=1730156, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/ad	A-MOZ-FIRE-201221/249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visories/mfsa2021-48/	
Exposure of Resource to Wrong Sphere	08-Dec-21	4.3	Microsoft introduced a new feature in Windows 10 known as Cloud Clipboard which, if enabled, will record data copied to the clipboard to the cloud, and make it available on other computers in certain scenarios. Applications that wish to prevent copied data from being recorded in Cloud History must use specific clipboard formats; and Firefox before versions 94 and ESR 91.3 did not implement them. This could have caused sensitive data to be recorded to a user's Microsoft account. *This bug only affects Firefox for Windows 10+ with Cloud Clipboard enabled. Other operating systems are unaffected.*. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38505**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://bugzilla.mozilla.org/show_bug.cgi?id=1730194, https://www.mozilla.org/security/advisories/mfsa2021-48/	A-MOZ-FIRE-201221/250
Improper Restriction of Rendered UI Layers or Frames	08-Dec-21	4.3	Through a series of navigations, Firefox could have entered fullscreen mode without notification or warning to the user. This could lead to spoofing attacks on the browser UI including phishing. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://bugzilla.mozilla.org/show_bug.cgi?id=1730750,	A-MOZ-FIRE-201221/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR < 91.3. **CVE ID : CVE-2021-38506**	https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/	
Origin Validation Error	08-Dec-21	4.3	The Opportunistic Encryption feature of HTTP2 (RFC 8164) allows a connection to be transparently upgraded to TLS while retaining the visual properties of an HTTP connection, including being same-origin with unencrypted connections on port 80. However, if a second encrypted port on the same IP address (e.g. port 8443) did not opt-in to opportunistic encryption; a network attacker could forward a connection from the browser to port 443 to port 8443, causing the browser to treat the content of port 8443 as same-origin with HTTP. This was resolved by disabling the Opportunistic Encryption feature, which had low usage. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38507**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://bugzilla.mozilla.org/show_bug.cgi?id=1730935, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/	A-MOZ-FIRE-201221/252
Improper Restriction	08-Dec-21	4.3	By displaying a form validity message in the correct	https://www.mozilla.org	A-MOZ-FIRE-201221/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Rendered UI Layers or Frames			location at the same time as a permission prompt (such as for geolocation), the validity message could have obscured the prompt, resulting in the user potentially being tricked into granting the permission. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38508**	/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/, https://bugzilla.mozilla.org/show_bug.cgi?id=1366818	
Improper Restriction of Rendered UI Layers or Frames	08-Dec-21	4.3	Due to an unusual sequence of attacker-controlled events, a Javascript alert() dialog with arbitrary (although unstyled) contents could be displayed over top an uncontrolled webpage of the attacker's choosing. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38509**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/, https://bugzilla.mozilla.org/show_bug.cgi?id=1718571	A-MOZ-FIRE-201221/254
Improper Neutralizatio	08-Dec-21	6.8	The executable file warning was not presented when	https://www.mozilla.org	A-MOZ-FIRE-201221/255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			downloading .inetloc files, which, due to a flaw in Mac OS, can run commands on a user's computer.*Note: This issue only affected Mac OS operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38510**	/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/, https://bugzilla.mozilla.org/show_bug.cgi?id=1731779	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	A Universal XSS vulnerability was present in Firefox for Android resulting from improper sanitization when processing a URL scanned from a QR code. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 94. **CVE ID : CVE-2021-43530**	https://www.mozilla.org/security/advisories/mfsa2021-48/	A-MOZ-FIRE-201221/256
Origin Validation Error	08-Dec-21	4.3	When a user loaded a Web Extensions context menu, the Web Extension could access the post-redirect URL of the element clicked. If the Web Extension lacked the WebRequest permission for the hosts involved in the redirect, this would be a same-origin-violation leaking	https://bugzilla.mozilla.org/show_bug.cgi?id=1659155, https://www.mozilla.org/security/advisories/mfsa2021-48/	A-MOZ-FIRE-201221/257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data the Web Extension should have access to. This was fixed to provide the pre-redirect URL. This is related to CVE-2021-43532 but in the context of Web Extensions. This vulnerability affects Firefox < 94. **CVE ID : CVE-2021-43531**		
URL Redirection to Untrusted Site ('Open Redirect')	08-Dec-21	5.8	The 'Copy Image Link' context menu action would copy the final image URL after redirects. By embedding an image that triggered authentication flows - in conjunction with a Content Security Policy that stopped a redirection chain in the middle - the final image URL could be one that contained an authentication token used to takeover a user account. If a website tricked a user into copy and pasting the image link back to the page, the page would be able to steal the authentication tokens. This was fixed by making the action return the original URL, before any redirects. This vulnerability affects Firefox < 94. **CVE ID : CVE-2021-43532**	https://bugzilla.mozilla.org/show_bug.cgi?id=1719203, https://www.mozilla.org/security/advisories/mfsa2021-48/	A-MOZ-FIRE-201221/258
N/A	08-Dec-21	4.3	When parsing internationalized domain names, high bits of the characters in the URLs were sometimes stripped, resulting in inconsistencies that could lead to user confusion or	https://bugzilla.mozilla.org/show_bug.cgi?id=1724233, https://www.mozilla.org	A-MOZ-FIRE-201221/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks such as phishing. This vulnerability affects Firefox < 94. **CVE ID : CVE-2021-43533**	/security/advisories/mfsa2021-48/	
Out-of-bounds Write	08-Dec-21	6.8	Mozilla developers and community members reported memory safety bugs present in Firefox 93 and Firefox ESR 91.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-43534**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/	A-MOZ-FIRE-201221/260
Use After Free	08-Dec-21	6.8	A use-after-free could have occured when an HTTP2 session object was released on a different thread, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 93, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-43535**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://bugzilla.mozilla.org/show_bug.cgi?id=1667102	A-MOZ-FIRE-201221/261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	08-Dec-21	4.3	Under certain circumstances, asynchronous functions could have caused a navigation to fail but expose the target URL. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43536**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	A-MOZ-FIRE-201221/262
Incorrect Type Conversion or Cast	08-Dec-21	6.8	An incorrect type conversion of sizes from 64bit to 32bit integers allowed an attacker to corrupt memory leading to a potentially exploitable crash. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43537**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/, https://bugzilla.mozilla.org/show_bug.cgi?id=1738237	A-MOZ-FIRE-201221/263
Concurrent Execution using Shared Resource with	08-Dec-21	4.3	By misusing a race in our notification code, an attacker could have forcefully hidden the notification for pages that had received full screen and	https://www.mozilla.org/security/advisories/mfsa2021-52/,	A-MOZ-FIRE-201221/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			pointer lock access, which could have been used for spoofing attacks. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43538**	https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/, https://bugzilla.mozilla.org/show_bug.cgi?id=1739091	
Use After Free	08-Dec-21	6.8	Failure to correctly record the location of live pointers across wasm instance calls resulted in a GC occurring within the call not tracing those live pointers. This could have led to a use-after-free causing a potentially exploitable crash. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43539**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://bugzilla.mozilla.org/show_bug.cgi?id=1739683, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	A-MOZ-FIRE-201221/265
Incorrect Permission Assignment for Critical Resource	08-Dec-21	4.3	WebExtensions with the correct permissions were able to create and install ServiceWorkers for third-party websites that would not	https://www.mozilla.org/security/advisories/mfsa2021-52/,	A-MOZ-FIRE-201221/266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have been uninstalled with the extension. This vulnerability affects Firefox < 95. **CVE ID : CVE-2021-43540**	https://bugzilla.mozilla.org/show_bug.cgi?id=1636629	
N/A	08-Dec-21	4.3	When invoking protocol handlers for external protocols, a supplied parameter URL containing spaces was not properly escaped. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43541**	https://bugzilla.mozilla.org/show_bug.cgi?id=1696685, https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	A-MOZ-FIRE-201221/267
Generation of Error Message Containing Sensitive Information	08-Dec-21	4.3	Using XMLHttpRequest, an attacker could have identified installed applications by probing error messages for loading external protocols. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43542**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/,	A-MOZ-FIRE-201221/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://bugzilla.mozilla.org/show_bug.cgi?id=1723281	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	Documents loaded with the CSP sandbox directive could have escaped the sandbox's script restriction by embedding additional content. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43543**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://bugzilla.mozilla.org/show_bug.cgi?id=1738418, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	A-MOZ-FIRE-201221/269
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	When receiving a URL through a SEND intent, Firefox would have searched for the text, but subsequent usages of the address bar might have caused the URL to load unintentionally, which could lead to XSS and spoofing attacks. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 95. **CVE ID : CVE-2021-43544**	https://www.mozilla.org/security/advisories/mfsa2021-52/	A-MOZ-FIRE-201221/270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Excessive Iteration	08-Dec-21	4.3	Using the Location API in a loop could have caused severe application hangs and crashes. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43545**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	A-MOZ-FIRE-201221/271
Improper Restriction of Rendered UI Layers or Frames	08-Dec-21	4.3	It was possible to recreate previous cursor spoofing attacks against users with a zoomed native cursor. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43546**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/, https://bugzilla.mozilla.org/show_bug.cgi?id=1737751	A-MOZ-FIRE-201221/272
firefox_esr					
Incorrect Authorization	08-Dec-21	7.5	The iframe sandbox rules were not correctly applied to XSLT stylesheets, allowing an iframe to bypass restrictions	https://www.mozilla.org/security/advisories/mfs	A-MOZ-FIRE-201221/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			such as executing scripts or navigating the top-level frame. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38503**	a2021-50/, https://bugzilla.mozilla.org/show_bug.cgi?id=1729517, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/	
Use After Free	08-Dec-21	7.5	When interacting with an HTML input element's file picker dialog with webkitdirectory set, a use-after-free could have resulted, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38504**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://bugzilla.mozilla.org/show_bug.cgi?id=1730156, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/	A-MOZ-FIRE-201221/274
Exposure of Resource to Wrong Sphere	08-Dec-21	4.3	Microsoft introduced a new feature in Windows 10 known as Cloud Clipboard which, if enabled, will record	https://www.mozilla.org/security/advisories/mfs	A-MOZ-FIRE-201221/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data copied to the clipboard to the cloud, and make it available on other computers in certain scenarios. Applications that wish to prevent copied data from being recorded in Cloud History must use specific clipboard formats; and Firefox before versions 94 and ESR 91.3 did not implement them. This could have caused sensitive data to be recorded to a user's Microsoft account. *This bug only affects Firefox for Windows 10+ with Cloud Clipboard enabled. Other operating systems are unaffected.*. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38505**	a2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://bugzilla.mozilla.org/show_bug.cgi?id=1730194, https://www.mozilla.org/security/advisories/mfsa2021-48/	
Improper Restriction of Rendered UI Layers or Frames	08-Dec-21	4.3	Through a series of navigations, Firefox could have entered fullscreen mode without notification or warning to the user. This could lead to spoofing attacks on the browser UI including phishing. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38506**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://bugzilla.mozilla.org/show_bug.cgi?id=1730750, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://ww	A-MOZ-FIRE-201221/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				w.mozilla.org /security/ad visories/mfs a2021-48/	
Origin Validation Error	08-Dec-21	4.3	The Opportunistic Encryption feature of HTTP2 (RFC 8164) allows a connection to be transparently upgraded to TLS while retaining the visual properties of an HTTP connection, including being same-origin with unencrypted connections on port 80. However, if a second encrypted port on the same IP address (e.g. port 8443) did not opt-in to opportunistic encryption; a network attacker could forward a connection from the browser to port 443 to port 8443, causing the browser to treat the content of port 8443 as same-origin with HTTP. This was resolved by disabling the Opportunistic Encryption feature, which had low usage. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38507**	https://ww w.mozilla.org /security/ad visories/mfs a2021-50/, https://bugz illa.mozilla.o rg/show_bug .cgi?id=1730 935, https://ww w.mozilla.org /security/ad visories/mfs a2021-49/, https://ww w.mozilla.org /security/ad visories/mfs a2021-48/	A-MOZ-FIRE-201221/277
Improper Restriction of Rendered UI Layers or Frames	08-Dec-21	4.3	By displaying a form validity message in the correct location at the same time as a permission prompt (such as for geolocation), the validity message could have obscured the prompt, resulting in the user potentially being tricked	https://ww w.mozilla.org /security/ad visories/mfs a2021-50/, https://ww w.mozilla.org /security/ad	A-MOZ-FIRE-201221/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			into granting the permission. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38508**	visories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/, https://bugzilla.mozilla.org/show_bug.cgi?id=1366818	
Improper Restriction of Rendered UI Layers or Frames	08-Dec-21	4.3	Due to an unusual sequence of attacker-controlled events, a Javascript alert() dialog with arbitrary (although unstyled) contents could be displayed over top an uncontrolled webpage of the attacker's choosing. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38509**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/, https://bugzilla.mozilla.org/show_bug.cgi?id=1718571	A-MOZ-FIRE-201221/279
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-21	6.8	The executable file warning was not presented when downloading .inetloc files, which, due to a flaw in Mac OS, can run commands on a user's computer.*Note: This issue only affected Mac OS operating systems. Other	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/ad	A-MOZ-FIRE-201221/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating systems are unaffected.*. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38510**	visories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/, https://bugzilla.mozilla.org/show_bug.cgi?id=1731779	
Out-of-bounds Write	08-Dec-21	6.8	Mozilla developers and community members reported memory safety bugs present in Firefox 93 and Firefox ESR 91.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-43534**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/	A-MOZ-FIRE-201221/281
Use After Free	08-Dec-21	6.8	A use-after-free could have occured when an HTTP2 session object was released on a different thread, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 93, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-43535**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/ad	A-MOZ-FIRE-201221/282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visories/mfsa2021-49/, https://bugzilla.mozilla.org/show_bug.cgi?id=1667102	
Exposure of Resource to Wrong Sphere	08-Dec-21	4.3	Under certain circumstances, asynchronous functions could have caused a navigation to fail but expose the target URL. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43536**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	A-MOZ-FIRE-201221/283
Incorrect Type Conversion or Cast	08-Dec-21	6.8	An incorrect type conversion of sizes from 64bit to 32bit integers allowed an attacker to corrupt memory leading to a potentially exploitable crash. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43537**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/, https://bugzilla.mozilla.org/show_bug	A-MOZ-FIRE-201221/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.cgi?id=1738237	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Dec-21	4.3	By misusing a race in our notification code, an attacker could have forcefully hidden the notification for pages that had received full screen and pointer lock access, which could have been used for spoofing attacks. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43538**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/, https://bugzilla.mozilla.org/show_bug.cgi?id=1739091	A-MOZ-FIRE-201221/285
Use After Free	08-Dec-21	6.8	Failure to correctly record the location of live pointers across wasm instance calls resulted in a GC occurring within the call not tracing those live pointers. This could have led to a use-after-free causing a potentially exploitable crash. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43539**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://bugzilla.mozilla.org/show_bug.cgi?id=1739683, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/ad	A-MOZ-FIRE-201221/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visories/mfsa2021-53/	
N/A	08-Dec-21	4.3	When invoking protocol handlers for external protocols, a supplied parameter URL containing spaces was not properly escaped. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43541**	https://bugzilla.mozilla.org/show_bug.cgi?id=1696685, https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	A-MOZ-FIRE-201221/287
Generation of Error Message Containing Sensitive Information	08-Dec-21	4.3	Using XMLHttpRequest, an attacker could have identified installed applications by probing error messages for loading external protocols. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43542**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/, https://bugzilla.mozilla.org/show_bug	A-MOZ-FIRE-201221/288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.cgi?id=1723281	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	Documents loaded with the CSP sandbox directive could have escaped the sandbox's script restriction by embedding additional content. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43543**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://bugzilla.mozilla.org/show_bug.cgi?id=1738418, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	A-MOZ-FIRE-201221/289
Excessive Iteration	08-Dec-21	4.3	Using the Location API in a loop could have caused severe application hangs and crashes. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43545**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	A-MOZ-FIRE-201221/290
Improper Restriction of Rendered	08-Dec-21	4.3	It was possible to recreate previous cursor spoofing attacks against users with a	https://www.mozilla.org/security/ad	A-MOZ-FIRE-201221/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
UI Layers or Frames			zoomed native cursor. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43546**	visories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/, https://bugzilla.mozilla.org/show_bug.cgi?id=1737751	
thunderbird					
Incorrect Authorization	08-Dec-21	7.5	The iframe sandbox rules were not correctly applied to XSLT stylesheets, allowing an iframe to bypass restrictions such as executing scripts or navigating the top-level frame. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38503**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://bugzilla.mozilla.org/show_bug.cgi?id=1729517, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/	A-MOZ-THUN-201221/292
Use After Free	08-Dec-21	7.5	When interacting with an HTML input element's file	https://www.mozilla.org	A-MOZ-THUN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			picker dialog with webkitdirectory set, a use-after-free could have resulted, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38504**	/security/advisories/mfsa2021-50/, https://bugzilla.mozilla.org/show_bug.cgi?id=1730156, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/	201221/293
Exposure of Resource to Wrong Sphere	08-Dec-21	4.3	Microsoft introduced a new feature in Windows 10 known as Cloud Clipboard which, if enabled, will record data copied to the clipboard to the cloud, and make it available on other computers in certain scenarios. Applications that wish to prevent copied data from being recorded in Cloud History must use specific clipboard formats; and Firefox before versions 94 and ESR 91.3 did not implement them. This could have caused sensitive data to be recorded to a user's Microsoft account. *This bug only affects Firefox for Windows 10+ with Cloud Clipboard enabled. Other operating systems are	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://bugzilla.mozilla.org/show_bug.cgi?id=1730194, https://www.mozilla.org/security/advisories/mfsa2021-48/	A-MOZ-THUN-201221/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unaffected.*. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38505**		
Improper Restriction of Rendered UI Layers or Frames	08-Dec-21	4.3	Through a series of navigations, Firefox could have entered fullscreen mode without notification or warning to the user. This could lead to spoofing attacks on the browser UI including phishing. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38506**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://bugzilla.mozilla.org/show_bug.cgi?id=1730750, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/	A-MOZ-THUN-201221/295
Origin Validation Error	08-Dec-21	4.3	The Opportunistic Encryption feature of HTTP2 (RFC 8164) allows a connection to be transparently upgraded to TLS while retaining the visual properties of an HTTP connection, including being same-origin with unencrypted connections on port 80. However, if a second encrypted port on the same IP address (e.g. port 8443) did not opt-in to opportunistic encryption; a network attacker could	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://bugzilla.mozilla.org/show_bug.cgi?id=1730935, https://www.mozilla.org/security/advisories/mfsa2021-49/,	A-MOZ-THUN-201221/296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			forward a connection from the browser to port 443 to port 8443, causing the browser to treat the content of port 8443 as same-origin with HTTP. This was resolved by disabling the Opportunistic Encryption feature, which had low usage. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38507**	https://www.mozilla.org/security/advisories/mfsa2021-48/	
Improper Restriction of Rendered UI Layers or Frames	08-Dec-21	4.3	By displaying a form validity message in the correct location at the same time as a permission prompt (such as for geolocation), the validity message could have obscured the prompt, resulting in the user potentially being tricked into granting the permission. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38508**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/, https://bugzilla.mozilla.org/show_bug.cgi?id=1366818	A-MOZ-THUN-201221/297
Improper Restriction of Rendered UI Layers or Frames	08-Dec-21	4.3	Due to an unusual sequence of attacker-controlled events, a Javascript alert() dialog with arbitrary (although unstyled) contents could be displayed over top an uncontrolled webpage of the	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org	A-MOZ-THUN-201221/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker's choosing. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38509**	/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/, https://bugzilla.mozilla.org/show_bug.cgi?id=1718571	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-21	6.8	The executable file warning was not presented when downloading .inetloc files, which, due to a flaw in Mac OS, can run commands on a user's computer.*Note: This issue only affected Mac OS operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38510**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/, https://bugzilla.mozilla.org/show_bug.cgi?id=1731779	A-MOZ-THUN-201221/299
Improper Privilege Management	08-Dec-21	4.3	Thunderbird unexpectedly enabled JavaScript in the composition area. The JavaScript execution context was limited to this area and did not receive chrome-level privileges, but could be used	https://www.mozilla.org/security/advisories/mfsa2021-54/, https://bugzilla.mozilla.o	A-MOZ-THUN-201221/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as a stepping stone to further an attack with other vulnerabilities. This vulnerability affects Thunderbird < 91.4.0. **CVE ID : CVE-2021-43528**	rg/show_bug.cgi?id=1742579	
Out-of-bounds Write	08-Dec-21	6.8	Mozilla developers and community members reported memory safety bugs present in Firefox 93 and Firefox ESR 91.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-43534**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://www.mozilla.org/security/advisories/mfsa2021-48/	A-MOZ-THUN-201221/301
Use After Free	08-Dec-21	6.8	A use-after-free could have occured when an HTTP2 session object was released on a different thread, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 93, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-43535**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://bugzilla.mozilla.org/show_bug.cgi?id=1667	A-MOZ-THUN-201221/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				102	
Exposure of Resource to Wrong Sphere	08-Dec-21	4.3	Under certain circumstances, asynchronous functions could have caused a navigation to fail but expose the target URL. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43536**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	A-MOZ-THUN-201221/303
Incorrect Type Conversion or Cast	08-Dec-21	6.8	An incorrect type conversion of sizes from 64bit to 32bit integers allowed an attacker to corrupt memory leading to a potentially exploitable crash. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43537**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/, https://bugzilla.mozilla.org/show_bug.cgi?id=1738237	A-MOZ-THUN-201221/304
Concurrent Execution using Shared Resource	08-Dec-21	4.3	By misusing a race in our notification code, an attacker could have forcefully hidden the notification for pages that	https://www.mozilla.org/security/advisories/mfs	A-MOZ-THUN-201221/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			had received full screen and pointer lock access, which could have been used for spoofing attacks. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43538**	a2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/, https://bugzilla.mozilla.org/show_bug.cgi?id=1739091	
Use After Free	08-Dec-21	6.8	Failure to correctly record the location of live pointers across wasm instance calls resulted in a GC occurring within the call not tracing those live pointers. This could have led to a use-after-free causing a potentially exploitable crash. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43539**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://bugzilla.mozilla.org/show_bug.cgi?id=1739683, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	A-MOZ-THUN-201221/306
N/A	08-Dec-21	4.3	When invoking protocol handlers for external protocols, a supplied parameter URL containing	https://bugzilla.mozilla.org/show_bug.cgi?id=1696	A-MOZ-THUN-201221/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			spaces was not properly escaped. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43541**	685, https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	
Generation of Error Message Containing Sensitive Information	08-Dec-21	4.3	Using XMLHttpRequest, an attacker could have identified installed applications by probing error messages for loading external protocols. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43542**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/, https://bugzilla.mozilla.org/show_bug.cgi?id=1723281	A-MOZ-THUN-201221/308
Improper Neutralization of Input During Web	08-Dec-21	4.3	Documents loaded with the CSP sandbox directive could have escaped the sandbox's script restriction by	https://www.mozilla.org/security/advisories/mfs	A-MOZ-THUN-201221/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			embedding additional content. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43543**	a2021-52/, https://bugzilla.mozilla.org/show_bug.cgi?id=1738418, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	
Excessive Iteration	08-Dec-21	4.3	Using the Location API in a loop could have caused severe application hangs and crashes. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43545**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfsa2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/	A-MOZ-THUN-201221/310
Improper Restriction of Rendered UI Layers or Frames	08-Dec-21	4.3	It was possible to recreate previous cursor spoofing attacks against users with a zoomed native cursor. This vulnerability affects Thunderbird < 91.4.0, Firefox ESR < 91.4.0, and Firefox < 95. **CVE ID : CVE-2021-43546**	https://www.mozilla.org/security/advisories/mfsa2021-52/, https://www.mozilla.org/security/advisories/mfs	A-MOZ-THUN-201221/311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				a2021-54/, https://www.mozilla.org/security/advisories/mfsa2021-53/, https://bugzilla.mozilla.org/show_bug.cgi?id=1737751	
nebulab					
solidus					
N/A	07-Dec-21	5	Solidus is a free, open-source ecommerce platform built on Rails. Versions of Solidus prior to 3.1.4, 3.0.4, and 2.11.13 have a denial of service vulnerability that could be exploited during a guest checkout. The regular expression used to validate a guest order's email was subject to exponential backtracking through a fragment like `a.a.` Versions 3.1.4, 3.0.4, and 2.11.13 have been patched to use a different regular expression. The maintainers added a check for email addresses that are no longer valid that will print information about any affected orders that exist. If a prompt upgrade is not an option, a workaround is available. It is possible to edit the file `config/application.rb` manually (with code provided by the maintainers	https://github.com/solidusio/solidus/security/advisories/GHSA-qxmr-qxh6-2cc9, https://github.com/solidusio/solidus/commit/9867153e01e3c3b898cdbced d7b43375ea922401	A-NEB-SOLI-201221/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the GitHub Security Advisory) to check email validity. **CVE ID : CVE-2021-43805**		
netty					
netty					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	09-Dec-21	4.3	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. Netty prior to version 4.1.7.1.Final skips control chars when they are present at the beginning / end of the header name. It should instead fail fast as these are not allowed by the spec and could lead to HTTP request smuggling. Failing to do the validation might cause netty to "sanitize" header names before it forward these to another remote system when used as proxy. This remote system can't see the invalid usage anymore, and therefore does not do the validation itself. Users should upgrade to version 4.1.7.1.Final to receive a patch. **CVE ID : CVE-2021-43797**	https://github.com/netty/netty/security/advisories/GHSA-wx5j-54mm-rqqq, https://github.com/netty/netty/commit/07aa6b5938a8b6ed7a6586e066400e2643897323	A-NET-NETT-201221/313
Nomachine					
cloud_server					
Integer Overflow or	07-Dec-21	7.2	NoMachine Cloud Server is affected by Integer Overflow.	N/A	A-NOM-CLOU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			IOCTL Handler 0x22001B in the NoMachine Cloud Server above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42979**		201221/314
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	NoMachine Cloud Server is affected by Buffer Overflow. IOCTL Handler 0x22001B in the NoMachine Cloud Server above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42980**	N/A	A-NOM-CLOU-201221/315
enterprise_client					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	NoMachine Enterprise Client is affected by Buffer Overflow. IOCTL Handler 0x22001B in the NoMachine Enterprise Client above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42983**	N/A	A-NOM-ENTE-201221/316
Integer	07-Dec-21	7.2	NoMachine Enterprise Client	N/A	A-NOM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			is affected by Integer Overflow. IOCTL Handler 0x22001B in the NoMachine Enterprise Client above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42986**		ENTE-201221/317
enterprise_desktop					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	NoMachine Enterprise Desktop is affected by Buffer Overflow. IOCTL Handler 0x22001B in the NoMachine Enterprise Desktop above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42976**	N/A	A-NOM-ENTE-201221/318
Integer Overflow or Wraparound	07-Dec-21	7.2	NoMachine Enterprise Desktop is affected by Integer Overflow. IOCTL Handler 0x22001B in the NoMachine Enterprise Desktop above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42977**	N/A	A-NOM-ENTE-201221/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
server					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	NoMachine Server is affected by Buffer Overflow. IOCTL Handler 0x22001B in the NoMachine Server above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42972**	N/A	A-NOM-SERV-201221/320
Integer Overflow or Wraparound	07-Dec-21	7.2	NoMachine Server is affected by Integer Overflow. IOCTL Handler 0x22001B in the NoMachine Server above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42973**	N/A	A-NOM-SERV-201221/321
nzedb_project					
nzedb					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-21	4.3	nZEDb v0.4.20 is affected by a Cross Site Scripting (XSS) vulnerability in www/pages/api.php. The exit function will terminate the script and print the message which has the input $_GET['t']. **CVE ID : CVE-2021-43686**	N/A	A-NZE-NZED-201221/322
okfn					
ckan					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	3.5	In CKAN, versions 2.9.0 to 2.9.3 are affected by a stored XSS vulnerability via SVG file upload of users' profile picture. This allows low privileged application users to store malicious scripts in their profile picture. These scripts are executed in a victim's browser when they open the malicious profile picture **CVE ID : CVE-2021-25967**	https://www.whitesourcesoftware.com/vulnerability-database/CVE-2021-25967	A-OKF-CKAN-201221/323
online_enrollment_management_system_project					
online_enrollment_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Dec-21	6.5	Authenticated Blind & Error-based SQL injection vulnerability was discovered in Online Enrollment Management System in PHP and PayPal Free Source Code 1.0, that allows attackers to obtain sensitive information and execute arbitrary SQL commands via IDNO parameter. **CVE ID : CVE-2021-40578**	N/A	A-ONL-ONLI-201221/324
openblas_project					
openblas					
Out-of-bounds Read	08-Dec-21	6.4	An out-of-bounds read flaw was found in the CLARRV, DLARRV, SLARRV, and ZLARRV functions in lapack through version 3.10.0, as also used in OpenBLAS before version 0.3.18. Specially crafted inputs passed to these functions could cause an	https://github.com/JuliaLang/julia/issues/42415, https://github.com/xianyi/OpenBLAS/commit/337b65133df17	A-OPE-OPEN-201221/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application using lapack to crash or possibly disclose portions of its memory. **CVE ID : CVE-2021-4048**	4796794871b3988cd03426e6d41, https://github.com/xianyi/OpenBLAS/commit/2be5ee3cca97a597f2ee2118808a2d5eacea050c	
opendesign					
drawings_explorer					
Out-of-bounds Write	05-Dec-21	6.8	An out-of-bounds write vulnerability exists when reading a TIF file using Open Design Alliance (ODA) Drawings Explorer before 2022.11. The specific issue exists after loading TIF files. Crafted data in a TIF file can trigger a write operation past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2021-44048**	https://www.opendesign.com/security-advisories	A-OPE-DRAW-201221/326
drawings_sdk					
Out-of-bounds Write	05-Dec-21	6.8	An out-of-bounds write vulnerability exists when reading a JPG file using Open Design Alliance Drawings SDK before 2022.11. The specific issue exists with parsing JPG files. Crafted data in a JPG (4 extraneous bytes before the marker 0xca) can trigger a write operation past	https://www.opendesign.com/security-advisories	A-OPE-DRAW-201221/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2021-44044**		
Out-of-bounds Write	05-Dec-21	6.8	An out-of-bounds write vulnerability exists when reading a DGN file using Open Design Alliance Drawings SDK before 2022.11. The specific issue exists within the parsing of DGN files. Crafted data in a DGN file and lack of proper validation for the XFAT sectors count can trigger a write operation past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2021-44045**	https://www.opendesign.com/security-advisories	A-OPE-DRAW-201221/328
Use After Free	05-Dec-21	6.8	A use-after-free vulnerability exists when reading a DWF/DWFX file using Open Design Alliance Drawings SDK before 2022.11. The specific issue exists with parsing DWF/DWFX files. Crafted data in a DWF/DWFX file and lack of proper validation of input data can trigger a write operation past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process.	https://www.opendesign.com/security-advisories	A-OPE-DRAW-201221/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-44047		
prc_sdk					
Out-of-bounds Write	05-Dec-21	6.8	An out-of-bounds write vulnerability exists when reading U3D files in Open Design Alliance PRC SDK before 2022.11. An unchecked return value of a function (verifying input data from a U3D file) leads to an out-of-bounds write. An attacker can leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2021-44046**	N/A	A-OPE-PRC_-201221/330
openwhyd					
openwhyd					
URL Redirection to Untrusted Site ('Open Redirect')	10-Dec-21	5.8	openwhyd is vulnerable to URL Redirection to Untrusted Site **CVE ID : CVE-2021-3829**	https://huntr.dev/bounties/6b8acb0c-8b5d-461e-9b46-b1bfb5a8ccdf, https://github.com/openwhyd/openwhyd/commit/3870793010 3dcba49d89d993f56bebd346069640	A-OPE-OPEN-201221/331
pdf.js_viewer_project					
pdf.js_viewer					
Improper Neutralizatio	06-Dec-21	3.5	The PDF.js Viewer WordPress plugin before 2.0.2 does not	N/A	A-PDF-PDF.-201221/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			escape some of its shortcode and Gutenberg Block attributes, which could allow users with a role as low as Contributor to to perform Cross-Site Scripting attacks **CVE ID : CVE-2021-24759**		
phpgurukul					
hostel_management_system					
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) vulnerability exits in hostel management system 2.1 via the name field in my-profile.php. Chaining to this both vulnerabilities leads to account takeover. **CVE ID : CVE-2021-43137**	N/A	A-PHP-HOST-201221/333
Pimcore					
pimcore					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-21	4.3	pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-4081**	https://github.com/pimcore/pimcore/commit/34ed0e050ff679b4b38414aef48ea1ff956f907a, https://huntr.dev/bounties/da173e66-76ba-4f98-b8fb-429aabf222d3	A-PIM-PIMC-201221/334
Cross-Site Request Forgery	10-Dec-21	4.3	pimcore is vulnerable to Cross-Site Request Forgery (CSRF)	https://github.com/pimcore/pimcore/	A-PIM-PIMC-201221/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			**CVE ID : CVE-2021-4082**	commit/3088cec7dc3cbc5a8b26f1269e398e799ee7ee28, https://huntr.dev/bounties/81838575-e170-41fb-b451-92c1c8aab092	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-21	4.3	pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-4084**	https://huntr.dev/bounties/dcb37f19-ba53-4498-b953-d21999279266, https://github.com/pimcore/pimcore/commit/3c2a14e676a57e5d77a16255965988eef48f9065	A-PIM-PIMC-201221/336
Pineapp					
mail_secure					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	PineApp - Mail Secure - Attacker sending a request to :/blocking.php?url=<script>alert(1)</script> and stealing cookies . **CVE ID : CVE-2021-36720**	N/A	A-PIN-MAIL-201221/337
Piwigo					
piwigo					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Dec-21	6.5	Piwigo v11.5 was discovered to contain a SQL injection vulnerability via the parameter pwg_token in /admin/batch_manager_global.php. **CVE ID : CVE-2021-40313**	N/A	A-PIW-PIWI-201221/338
Plex					
media_server					
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Dec-21	6.9	An issue was discovered in Plex Media Server through 1.24.4.5081-e362dc1ee. An attacker (with a foothold in a endpoint via a low-privileged user account) can access the exposed RPC service of the update service component. This RPC functionality allows the attacker to interact with the RPC functionality and execute code from a path of his choice (local, or remote via SMB) because of a TOCTOU race condition. This code execution is in the context of the Plex update service (which runs as SYSTEM). **CVE ID : CVE-2021-42835**	https://forums.plex.tv/t/security-regarding-cve-2021-42835/761510, https://www.plex.tv/media-server-downloads/	A-PLE-MEDI-201221/339
Pluck-cms					
pluck					
Unrestricted Upload of File with Dangerous Type	10-Dec-21	7.5	In Pluck-4.7.15 admin background a remote command execution vulnerability exists when uploading files.	N/A	A-PLU-PLUC-201221/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-27984		
Session Fixation	10-Dec-21	5	Session Fixation vulnerability in login.php in Pluck-CMS Pluck 4.7.15 allows an attacker to sustain unauthorized access to the platform. Because Pluck does not invalidate prior sessions after a password change, access can be sustained even after an administrator performs regular remediation attempts such as resetting their password. **CVE ID : CVE-2021-31745**	N/A	A-PLU-PLUC-201221/341
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Dec-21	7.5	Zip Slip vulnerability in Pluck-CMS Pluck 4.7.15 allows an attacker to upload specially crafted zip files, resulting in directory traversal and potentially arbitrary code execution. **CVE ID : CVE-2021-31746**	N/A	A-PLU-PLUC-201221/342
Improper Certificate Validation	10-Dec-21	5.8	Missing SSL Certificate Validation issue exists in Pluck 4.7.15 in update_applet.php, which could lead to man-in-the-middle attacks. **CVE ID : CVE-2021-31747**	N/A	A-PLU-PLUC-201221/343
Prestashop					
prestashop					
Improper Neutralization of Special Elements used in an SQL	07-Dec-21	7.5	PrestaShop is an Open Source e-commerce web application. Versions of PrestaShop prior to 1.7.8.2 are vulnerable to blind SQL injection using search filters with `orderBy`	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-6xxj-	A-PRE-PRES-201221/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			and `sortOrder` parameters. The problem is fixed in version 1.7.8.2. **CVE ID : CVE-2021-43789**	gcjq-wgf4	
profilepress					
loginwp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-21	4.3	The LoginWP (Formerly Peter's Login Redirect) WordPress plugin before 3.0.0.5 does not sanitise and escape the rul_login_url and rul_logout_url parameter before outputting them back in attributes in an admin page, leading to a Reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24939**	N/A	A-PRO-LOGI-201221/345
Redhat					
ceph_storage					
Out-of-bounds Read	08-Dec-21	6.4	An out-of-bounds read flaw was found in the CLARRV, DLARRV, SLARRV, and ZLARRV functions in lapack through version 3.10.0, as also used in OpenBLAS before version 0.3.18. Specially crafted inputs passed to these functions could cause an application using lapack to crash or possibly disclose portions of its memory. **CVE ID : CVE-2021-4048**	https://github.com/JuliaLang/julia/issues/42415, https://github.com/xianyi/OpenBLAS/commit/337b65133df174796794871b3988cd03426e6d41, https://github.com/xianyi/OpenBLAS/commit/2be5ee3cca97a597f2ee2118808a2d5eacea	A-RED-CEPH-201221/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				050c	
openshift_container_storage					
Out-of-bounds Read	08-Dec-21	6.4	An out-of-bounds read flaw was found in the CLARRV, DLARRV, SLARRV, and ZLARRV functions in lapack through version 3.10.0, as also used in OpenBLAS before version 0.3.18. Specially crafted inputs passed to these functions could cause an application using lapack to crash or possibly disclose portions of its memory. **CVE ID : CVE-2021-4048**	https://github.com/JuliaLang/julia/issues/42415, https://github.com/xianyi/OpenBLAS/commit/337b65133df174796794871b3988cd03426e6d41, https://github.com/xianyi/OpenBLAS/commit/2be5ee3cca97a597f2ee2118808a2d5eacea050c	A-RED-OPEN-201221/347
openshift_data_foundation					
Out-of-bounds Read	08-Dec-21	6.4	An out-of-bounds read flaw was found in the CLARRV, DLARRV, SLARRV, and ZLARRV functions in lapack through version 3.10.0, as also used in OpenBLAS before version 0.3.18. Specially crafted inputs passed to these functions could cause an application using lapack to crash or possibly disclose portions of its memory. **CVE ID : CVE-2021-4048**	https://github.com/JuliaLang/julia/issues/42415, https://github.com/xianyi/OpenBLAS/commit/337b65133df174796794871b3988cd03426e6d41, https://github.com/xianyi/OpenBLAS/commit/2be5ee3cca97a5	A-RED-OPEN-201221/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				97f2ee2118808a2d5eacea050c	
reputeinfosystems					
contact_form\\,_survey_\\&_popup_form_plugin_for_wordpress_-_arforms_form_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-21	3.5	The Contact Form, Survey & Popup Form Plugin for WordPress plugin before 1.5 does not properly sanitize some of its settings allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24718**	N/A	A-REP-CONT-201221/349
requarks					
wiki.js					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Dec-21	4.3	Wiki.js is a wiki app built on Node.js. Prior to version 2.5.254, directory traversal outside of Wiki.js context is possible when a storage module with local asset cache fetching is enabled on a Windows host. A malicious user can potentially read any file on the file system by crafting a special URL that allows for directory traversal. This is only possible on a Wiki.js server running on Windows, when a storage module implementing local asset cache (e.g Local File System or Git) is enabled and that no web application firewall solution (e.g. cloudflare) strips potentially	https://github.com/Requarks/wiki/commit/414033de9dff66a327e3f3243234852f468a9d85, https://github.com/Requarks/wiki/security/advisories/GHSA-r363-73gj-6j25	A-REQ-WIKI-201221/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious URLs. Commit number 414033de9dff66a327e3f3243234852f468a9d85 fixes this vulnerability by sanitizing the path before it is passed on to the storage module. The sanitization step removes any windows directory traversal sequences from the path. As a workaround, disable any storage module with local asset caching capabilities (Local File System, Git). **CVE ID : CVE-2021-43800**		
roundupwp					
registrations_for_the_events_calendar					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Dec-21	7.5	The Registrations for the Events Calendar WordPress plugin before 2.7.6 does not sanitise and escape the event_id in the rtec_send_unregister_link AJAX action (available to both unauthenticated and authenticated users) before using it in a SQL statement, leading to an unauthenticated SQL injection. **CVE ID : CVE-2021-24943**	N/A	A-ROU-REGI-201221/351
Samsung					
contacts					
Insecure Storage of Sensitive Information	08-Dec-21	2.1	Insecure storage of device information in Contacts prior to version 12.7.05.24 allows attacker to get Samsung Account ID. **CVE ID : CVE-2021-25524**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=	A-SAM-CONT-201221/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				12	
dialer					
Insecure Storage of Sensitive Information	08-Dec-21	2.1	Insecure storage of device information in Samsung Dialer prior to version 12.7.05.24 allows attacker to get Samsung Account ID. **CVE ID : CVE-2021-25523**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=12	A-SAM-DIAL-201221/353
internet					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	Insecure caller check and input validation vulnerabilities in SearchKeyword deeplink logic prior to Samsung Internet 16.0.2 allows unstrusted applications to execute script codes in Samsung Internet. **CVE ID : CVE-2021-25520**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=12	A-SAM-INTE-201221/354
Files or Directories Accessible to External Parties	08-Dec-21	2.1	Insecure caller check in sharevia deeplink logic prior to Samsung Internet 16.0.2 allows unstrusted applications to get current tab URL in Samsung Internet. **CVE ID : CVE-2021-25521**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=12	A-SAM-INTE-201221/355
pay					
Improper Check for Unusual or Exceptional Conditions	08-Dec-21	3.3	Improper check or handling of exception conditions vulnerability in Samsung Pay (US only) prior to version 4.0.65 allows attacker to use NFC without user recognition. **CVE ID : CVE-2021-25525**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=12	A-SAM-PAY-201221/356
smart_capture					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insecure Storage of Sensitive Information	08-Dec-21	2.1	Insecure storage of sensitive information vulnerability in Smart Capture prior to version 4.8.02.10 allows attacker to access victim's captured images without permission. **CVE ID : CVE-2021-25522**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=12	A-SAM-SMAR-201221/357
sey_project					
sey					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	10-Dec-21	7.5	All versions of package sey are vulnerable to Prototype Pollution via the deepmerge() function. **CVE ID : CVE-2021-23663**	https://snyk.io/vuln/SNYK-JS-SEY-1727592	A-SEY-SEY-201221/358
Shopex					
ecshop					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-21	7.5	ecshop v2.7.3 is affected by a SQL injection vulnerability in shopex\ecshop\upload\api\client\api.php. **CVE ID : CVE-2021-43679**	N/A	A-SHO-ECSH-201221/359
showdoc					
showdoc					
URL Redirection to Untrusted Site ('Open Redirect')	01-Dec-21	5.8	showdoc is vulnerable to URL Redirection to Untrusted Site **CVE ID : CVE-2021-3989**	https://github.com/star7th/showdoc/commit/335afc7ed6d6627c3d0434aa9acc168c771	A-SHO-SHOW-201221/360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				17614, https://hunt r.dev/bounti es/ffc61eff-efea-42c5-92c2-e043fdf904d5	
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	01-Dec-21	4.3	showdoc is vulnerable to Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) **CVE ID : CVE-2021-3990**	https://github.com/star7th/showdoc/commit/a9886f26c08225e0adca75c67dfca3f7c42b87d0, https://hunt r.dev/bounti es/0680067d-56a7-4412-b06e-a267e850ae9f	A-SHO-SHOW-201221/361
Cross-Site Request Forgery (CSRF)	01-Dec-21	4.3	showdoc is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-3993**	https://hunt r.dev/bounti es/0aa84736-139b-4ae7-becf-604f7f60b1c9, https://github.com/star7th/showdoc/commit/654e871a3923e79076818a9a03533fe88222c871	A-SHO-SHOW-201221/362
URL Redirection	03-Dec-21	5.8	showdoc is vulnerable to URL Redirection to Untrusted Site	https://hunt r.dev/bounti	A-SHO-SHOW-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to Untrusted Site ('Open Redirect')			**CVE ID : CVE-2021-4000**	es/e4d803e0-3104-432c-80b3-34bc453c8962, https://github.com/star7th/showdoc/commit/c7f10033eba5f2b5a537f9af9ba2379138e67138	201221/363
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	showdoc is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-4017**	https://huntr.dev/bounties/1d8439e8-b3f7-40f8-8b30-f9cb05ff2bcd, https://github.com/star7th/showdoc/commit/654e871a3923e79076818a9a03533fe88222c871	A-SHO-SHOW-201221/364
Siemens					
jt_open_toolkit					
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute code in the context of the current process. (ZDI-CAN-14829) **CVE ID : CVE-2021-44430**		
Out-of-bounds Read	14-Dec-21	4.3	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14841) **CVE ID : CVE-2021-44431**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/366
Stack-based Buffer Overflow	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to stack based buffer overflow while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14845) **CVE ID : CVE-2021-44432**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/367
Use After Free	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0).	https://cert-portal.siemens.com/productcert/pdf/	A-SIE-JT_O-201221/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			JTTK library in affected products contains a use after free vulnerability that could be triggered while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14900) **CVE ID : CVE-2021-44433**	ssa-802578.pdf	
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14902, ZDI-CAN-14866) **CVE ID : CVE-2021-44434**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/369
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to stack based buffer overflow while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14903) **CVE ID : CVE-2021-44435**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Dec-21	4.3	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14905) **CVE ID : CVE-2021-44436**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/371
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14906) **CVE ID : CVE-2021-44437**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/372
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14907) **CVE ID : CVE-2021-44438**		
Out-of-bounds Read	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14908) **CVE ID : CVE-2021-44439**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/374
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to memory corruption condition while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14912) **CVE ID : CVE-2021-44440**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/375
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK	https://cert-portal.siemens.com/prod	A-SIE-JT_O-201221/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14913) **CVE ID : CVE-2021-44441**	uctcert/pdf/ssa-802578.pdf	
Heap-based Buffer Overflow	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14995) **CVE ID : CVE-2021-44442**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/377
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15039)	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-44443		
Out-of-bounds Read	14-Dec-21	4.3	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15052) **CVE ID : CVE-2021-44444**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/379
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15054) **CVE ID : CVE-2021-44445**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_O-201221/380
Use After Free	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.0.3.0), JTTK (All versions < V11.0.3.0). JTTK library in affected products contains a use-after-free vulnerability that could	https://cert-portal.siemens.com/productcert/pdf/ssa-352143.pdf	A-SIE-JT_O-201221/381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be triggered while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14911) **CVE ID : CVE-2021-44447**		
Out-of-bounds Read	14-Dec-21	4.3	A vulnerability has been identified in JT Utilities (All versions < V13.0.3.0), JTTK (All versions < V11.0.3.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14843, ZDI-CAN-15051) **CVE ID : CVE-2021-44448**	https://cert-portal.siemens.com/productcert/pdf/ssa-352143.pdf	A-SIE-JT_O-201221/382
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V12.8.1.1), JTTK (All versions < V10.8.1.1). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14830) **CVE ID : CVE-2021-44449**	https://cert-portal.siemens.com/productcert/pdf/ssa-396621.pdf	A-SIE-JT_O-201221/383
Out-of-bounds Read	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V12.8.1.1), JTTK	https://cert-portal.siemens.com/prod	A-SIE-JT_O-201221/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V10.8.1.1). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15055, ZDI-CAN-14915, ZDI-CAN-14865) **CVE ID : CVE-2021-44450**	uctcert/pdf/ssa-396621.pdf	
jt_utilities					
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14829) **CVE ID : CVE-2021-44430**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/385
Out-of-bounds Read	14-Dec-21	4.3	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14841) **CVE ID : CVE-2021-44431**		
Stack-based Buffer Overflow	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to stack based buffer overflow while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14845) **CVE ID : CVE-2021-44432**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/387
Use After Free	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains a use after free vulnerability that could be triggered while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14900) **CVE ID : CVE-2021-44433**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/388
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected	https://cert-portal.siemens.com/productcert/pdf/ssa-	A-SIE-JT_U-201221/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14902, ZDI-CAN-14866) **CVE ID : CVE-2021-44434**	802578.pdf	
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to stack based buffer overflow while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14903) **CVE ID : CVE-2021-44435**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/390
Out-of-bounds Read	14-Dec-21	4.3	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14905)	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-44436		
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14906) **CVE ID : CVE-2021-44437**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/392
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14907) **CVE ID : CVE-2021-44438**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/393
Out-of-bounds Read	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14908) **CVE ID : CVE-2021-44439**		
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to memory corruption condition while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14912) **CVE ID : CVE-2021-44440**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/395
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14913) **CVE ID : CVE-2021-44441**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/396
Heap-based Buffer Overflow	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK	https://cert-portal.siemens.com/prod	A-SIE-JT_U-201221/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14995) **CVE ID : CVE-2021-44442**	uctcert/pdf/ssa-802578.pdf	
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15039) **CVE ID : CVE-2021-44443**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/398
Out-of-bounds Read	14-Dec-21	4.3	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CAN-15052) **CVE ID : CVE-2021-44444**		
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15054) **CVE ID : CVE-2021-44445**	https://cert-portal.siemens.com/productcert/pdf/ssa-802578.pdf	A-SIE-JT_U-201221/400
Use After Free	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V13.0.3.0), JTTK (All versions < V11.0.3.0). JTTK library in affected products contains a use-after-free vulnerability that could be triggered while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14911) **CVE ID : CVE-2021-44447**	https://cert-portal.siemens.com/productcert/pdf/ssa-352143.pdf	A-SIE-JT_U-201221/401
Out-of-bounds Read	14-Dec-21	4.3	A vulnerability has been identified in JT Utilities (All versions < V13.0.3.0), JTTK (All versions < V11.0.3.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer	https://cert-portal.siemens.com/productcert/pdf/ssa-352143.pdf	A-SIE-JT_U-201221/402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14843, ZDI-CAN-15051) **CVE ID : CVE-2021-44448**		
Out-of-bounds Write	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V12.8.1.1), JTTK (All versions < V10.8.1.1). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14830) **CVE ID : CVE-2021-44449**	https://cert-portal.siemens.com/productcert/pdf/ssa-396621.pdf	A-SIE-JT_U-201221/403
Out-of-bounds Read	14-Dec-21	6.8	A vulnerability has been identified in JT Utilities (All versions < V12.8.1.1), JTTK (All versions < V10.8.1.1). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15055, ZDI-CAN-14915, ZDI-CAN-14865) **CVE ID : CVE-2021-44450**	https://cert-portal.siemens.com/productcert/pdf/ssa-396621.pdf	A-SIE-JT_U-201221/404
snipeitapp					
snipe-it					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	3.5	snipe-it is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-4018**	https://hunter.dev/bounties/c14395f6-bf0d-4b06-b4d1-b509d8a99b54, https://github.com/snipe/snipe-it/commit/ff81e6d5366c2cfb15618793ad919ae4cbb3ac57	A-SNI-SNIP-201221/405
Server-Side Request Forgery (SSRF)	06-Dec-21	6.5	snipe-it is vulnerable to Server-Side Request Forgery (SSRF) **CVE ID : CVE-2021-4075**	https://github.com/snipe/snipe-it/commit/4612b9e711b3ff5d2bcddbec5b18866d25f8e34e, https://hunter.dev/bounties/4386fd8b-8c80-42bb-87b8-b506c46597de	A-SNI-SNIP-201221/406
Incorrect Authorization	10-Dec-21	4	snipe-it is vulnerable to Improper Access Control **CVE ID : CVE-2021-4089**	https://hunter.dev/bounties/19453ef1-4d77-4cff-b7e8-1bc8f3af0862, https://github.com/snipe/snipe-	A-SNI-SNIP-201221/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				it/commit/1699c09758e56f740437674a8d6ba36443399f24	
soflyy					
wp_all_import					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-21	3.5	The Import any XML or CSV File to WordPress plugin before 3.6.3 does not escape the Import's Title and Unique Identifier fields before outputting them in admin pages, which could allow high privilege users to perform Cross-Site attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24714**	N/A	A-SOF-WP_A-201221/408
Solarwinds					
serv-u					
Cross-Site Request Forgery (CSRF)	06-Dec-21	6.8	Serv-U server responds with valid CSRFToken when the request contains only Session. **CVE ID : CVE-2021-35242**	https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_15-2-5_release_notes.htm	A-SOL-SERV-201221/409
Improper Privilege Management	06-Dec-21	6.8	When a user has admin rights in Serv-U Console, the user can move, create and delete any files are able to be accessed on the Serv-U host machine. **CVE ID : CVE-2021-35245**	https://documentation.solarwinds.com/en/success_center/servu/content/release_notes	A-SOL-SERV-201221/410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/servu_15-2-5_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/CVE-2021-35245	
Sonicwall					
global_vpn_client					
Uncontrolled Search Path Element	08-Dec-21	6.9	SonicWall Global VPN client version 4.10.6 (32-bit and 64-bit) and earlier have a DLL Search Order Hijacking vulnerability. Successful exploitation via a local attacker could result in remote code execution in the target system. **CVE ID : CVE-2021-20047**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0025	A-SON-GLOB-201221/411
squaredup					
squaredup					
Server-Side Request Forgery (SSRF)	06-Dec-21	7.5	An SSRF issue was discovered in SquaredUp for SCOM 5.2.1.6654. **CVE ID : CVE-2021-40091**	https://support.squaredup.com/hc/en-us/articles/441065639412 9-CVE-2021-40091-SSRF-issue, https://support.squaredup.com	A-SQU-SQUA-201221/412
Improper	07-Dec-21	3.5	A cross-site scripting (XSS)	https://supp	A-SQU-SQUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			vulnerability in Image Tile in SquaredUp for SCOM 5.2.1.6654 allows remote attackers to inject arbitrary web script or HTML via an SVG file. **CVE ID : CVE-2021-40092**	ort.squaredup.com/hc/en-us/articles/44106354172 33-CVE-2021-40092-Stored-cross-site-scripting-Image-tile-, https://support.squaredup.com	201221/413
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-21	3.5	A cross-site scripting (XSS) vulnerability in integration configuration in SquaredUp for SCOM 5.2.1.6654 allows remote attackers to inject arbitrary web script or HTML via dashboard actions. **CVE ID : CVE-2021-40093**	https://support.squaredup.com/hc/en-us/articles/44106354182 57-CVE-2021-40093-Stored-cross-site-scripting-Action-Buttons-, https://support.squaredup.com	A-SQU-SQUA-201221/414
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-21	3.5	A DOM-based XSS vulnerability affects SquaredUp for SCOM 5.2.1.6654. If successfully exploited, this vulnerability may allow attackers to inject malicious code into a user's device. **CVE ID : CVE-2021-40094**	https://support.squaredup.com/hc/en-us/articles/44106563955 37-CVE-2021-40094-DOM-based-stored-cross-	A-SQU-SQUA-201221/415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				site-scripting, https://support.squaredup.com	
N/A	07-Dec-21	4	An issue was discovered in SquaredUp for SCOM 5.2.1.6654. The Download Log feature in System / Maintenance was susceptible to a local file inclusion vulnerability (when processing remote input in the log files downloaded by an authenticated administrator user), leading to the ability to read arbitrary files on the server filesystems. **CVE ID : CVE-2021-40095**	https://support.squaredup.com/hc/en-us/articles/441063541915 3-CVE-2021-40095-Reading-arbitrary-files, https://support.squaredup.com	A-SQU-SQUA-201221/416
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-21	3.5	A cross-site scripting (XSS) vulnerability in integration configuration in SquaredUp for SCOM 5.2.1.6654 allows remote attackers to inject arbitrary web script or HTML via modification of the authorisationUrl in some integration configurations. **CVE ID : CVE-2021-40096**	https://support.squaredup.com, https://support.squaredup.com/hc/en-us/articles/441065639681 7-CVE-2021-40096-Stored-cross-site-scripting-provider-configuration-	A-SQU-SQUA-201221/417
SUN					
ehrd					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Dec-21	7.8	Sunnet eHRD has inadequate filtering for special characters in URLs, which allows a remote attacker to perform path traversal attacks without authentication, access restricted paths and download system files. **CVE ID : CVE-2021-43358**	https://www.twcert.org.tw/tw/cp-132-5353-4ebee-1.html	A-SUN-EHRD-201221/418
Incorrect Permission Assignment for Critical Resource	01-Dec-21	9	Sunnet eHRD has broken access control vulnerability, which allows a remote attacker to access account management page after being authenticated as a general user, then perform privilege escalation to execute arbitrary code and control the system or interrupt services. **CVE ID : CVE-2021-43359**	https://www.twcert.org.tw/tw/cp-132-5354-0aac0-1.html	A-SUN-EHRD-201221/419
Deserialization of Untrusted Data	01-Dec-21	9	Sunnet eHRD e-mail delivery task schedule's serialization function has inadequate input object validation and restriction, which allows a post-authenticated remote attacker with database access privilege, to execute arbitrary code and control the system or interrupt services. **CVE ID : CVE-2021-43360**	https://www.twcert.org.tw/tw/cp-132-5355-6e339-1.html	A-SUN-EHRD-201221/420
swoole					
swoole_php_framework					
Improper Limitation of a Pathname to a	03-Dec-21	7.5	matyhtf framework v3.0.5 is affected by a path manipulation vulnerability in Smarty.class.php.	N/A	A-SWO-SWOO-201221/421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			**CVE ID : CVE-2021-43676**		
Synel					
eharmonynew					
Insertion of Sensitive Information into Log File	08-Dec-21	6.8	SYNEL - eharmonynew / Synel Reports - The attacker can log in to the system with default credentials and export a report of eharmony system with sensetive data (Employee name, Employee ID number, Working hours etc') The vulnerabilety has been addressed and fixed on version 11. Default credentials , Security miscommunication , Sensetive data exposure vulnerability in Synel Reports of SYNEL eharmonynew, Synel Reports allows an attacker to log into the system with default credentials. This issue affects: SYNEL eharmonynew, Synel Reports 8.0.2 version 11 and prior versions. **CVE ID : CVE-2021-36718**	N/A	A-SYN-EHAR-201221/422
synel_reports					
Insertion of Sensitive Information into Log File	08-Dec-21	6.8	SYNEL - eharmonynew / Synel Reports - The attacker can log in to the system with default credentials and export a report of eharmony system with sensetive data (Employee name, Employee ID number, Working hours	N/A	A-SYN-SYNE-201221/423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			etc') The vulnerabilety has been addressed and fixed on version 11. Default credentials , Security miscommunication , Sensetive data exposure vulnerability in Synel Reports of SYNEL eharmonynew, Synel Reports allows an attacker to log into the system with default credentials. This issue affects: SYNEL eharmonynew, Synel Reports 8.0.2 version 11 and prior versions. **CVE ID : CVE-2021-36718**		
taogogo					
taocms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-21	6.5	Taocms v2.5Beta5 was discovered to contain a blind SQL injection vulnerability via the function Article Search. **CVE ID : CVE-2021-25783**	N/A	A-TAO-TAOC-201221/424
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-21	6.5	Taocms v2.5Beta5 was discovered to contain a blind SQL injection vulnerability via the function Edit Article. **CVE ID : CVE-2021-25784**	N/A	A-TAO-TAOC-201221/425
Improper Neutralization of Input	02-Dec-21	3.5	Taocms v2.5Beta5 was discovered to contain a cross-site scripting (XSS)	N/A	A-TAO-TAOC-201221/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerability via the component Management column. **CVE ID : CVE-2021-25785**		
tawk					
tawk.to_live_chat					
Missing Authorization	06-Dec-21	6	The Tawk.To Live Chat WordPress plugin before 0.6.0 does not have capability and CSRF checks in the tawkto_setwidget and tawkto_removewidget AJAX actions, available to any authenticated user. The first one allows low-privileged users (including simple subscribers) to change the 'tawkto-embed-widget-page-id' and 'tawkto-embed-widget-widget-id' parameters. Any authenticated user can thus link the vulnerable website to their own Tawk.to instance. Consequently, they will be able to monitor the vulnerable website and interact with its visitors (receive contact messages, answer, ...). They will also be able to display an arbitrary Knowledge Base. The second one will remove the live chat widget from pages. **CVE ID : CVE-2021-24914**	N/A	A-TAW-TAWK-201221/427
thinkphp					
thinkphp					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	06-Dec-21	7.5	ThinkPHP v6.0.8 was discovered to contain a deserialization vulnerability via the component vendor\league\flysystem-cached-adapter\src\Storage\Adapter.php. **CVE ID : CVE-2021-36564**	N/A	A-THI-THIN-201221/428
Deserialization of Untrusted Data	06-Dec-21	10	ThinkPHP v6.0.8 was discovered to contain a deserialization vulnerability via the component League\Flysystem\Cached\Storage\AbstractCache. **CVE ID : CVE-2021-36567**	https://github.com/top-think/framework/issues/2561	A-THI-THIN-201221/429
thinkphp-bjyblog_project					
thinkphp-bjyblog					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-21	4.3	thinkphp-bjyblog (last update Jun 4 2021) is affected by a Cross Site Scripting (XSS) vulnerability in AdminBaseController.class.php. The exit function terminates the script and prints a message to the user that contains $_SERVER['HTTP_HOST']. **CVE ID : CVE-2021-43682**	N/A	A-THI-THIN-201221/430
thinkup					
thinkup					
Improper Limitation of a Pathname to a Restricted Directory ('Path	03-Dec-21	7.5	** UNSUPPORTED WHEN ASSIGNED ** ThinkUp 2.0-beta.10 is affected by a path manipulation vulnerability in Smarty.class.php. NOTE: This vulnerability only affects products that are no longer	N/A	A-THI-THIN-201221/431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			supported by the maintainer. **CVE ID : CVE-2021-43674**		
tianocore					
edk2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Dec-21	6.8	NetworkPkg/IScsiDxe has remotely exploitable buffer overflows. **CVE ID : CVE-2021-38575**	https://bugzilla.tianocore.org/show_bug.cgi?id=3356	A-TIA-EDK2-201221/432
tiny					
plupload					
Unrestricted Upload of File with Dangerous Type	03-Dec-21	6.8	This affects the package plupload before 2.3.9. A file name containing JavaScript code could be uploaded and run. An attacker would need to trick a user to upload this kind of file. **CVE ID : CVE-2021-23562**	https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBMOXIECODE-2306664, https://github.com/moxiecode/plupload/commit/d12175d4b5fa799b994ee1bb17bfbeec55b386fb, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-2306665, https://snyk.io/vuln/SNYK-JS-PLUPLOAD-	A-TIN-PLUP-201221/433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1583909	
tmate					
tmate-ssh-server					
Improper Preservation of Permissions	07-Dec-21	4.4	World-writable permissions on the /tmp/tmate/sessions directory in tmate-ssh-server 2.3.0 allow a local attacker to compromise the integrity of session handling, or obtain the read-write session ID from a read-only session symlink in this directory. **CVE ID : CVE-2021-44512**	https://github.com/tmate-io/tmate-ssh-server/commit/1c020d1f5ca462f5b150b46a027aaa1bbe3c9596	A-TMA-TMAT-201221/434
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	07-Dec-21	4.4	Insecure creation of temporary directories in tmate-ssh-server 2.3.0 allows a local attacker to compromise the integrity of session handling. **CVE ID : CVE-2021-44513**	https://github.com/tmate-io/tmate-ssh-server/commit/1c020d1f5ca462f5b150b46a027aaa1bbe3c9596	A-TMA-TMAT-201221/435
Trendmicro					
antivirus\\+_security					
Files or Directories Accessible to External Parties	03-Dec-21	2.1	Trend Micro Security 2021 v17.0 (Consumer) contains a vulnerability that allows files inside the protected folder to be modified without any detection. **CVE ID : CVE-2021-43772**	https://helpcenter.trendmicro.com/en-us/article/tmka-10855	A-TRE-ANTI-201221/436
apex_one					
Reachable Assertion	03-Dec-21	2.1	A reachable assertion vulnerability in Trend Micro Apex One could allow an attacker to crash the program	https://success.trendmicro.com/solution/0002892	A-TRE-APEX-201221/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on affected installations, leading to a denial-of-service (DoS). Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-44022**	29	
internet_security					
Files or Directories Accessible to External Parties	03-Dec-21	2.1	Trend Micro Security 2021 v17.0 (Consumer) contains a vulnerability that allows files inside the protected folder to be modified without any detection. **CVE ID : CVE-2021-43772**	https://helpcenter.trendmicro.com/en-us/article/tmka-10855	A-TRE-INTE-201221/438
maximum_security					
Files or Directories Accessible to External Parties	03-Dec-21	2.1	Trend Micro Security 2021 v17.0 (Consumer) contains a vulnerability that allows files inside the protected folder to be modified without any detection. **CVE ID : CVE-2021-43772**	https://helpcenter.trendmicro.com/en-us/article/tmka-10855	A-TRE-MAXI-201221/439
premium_security					
Files or Directories Accessible to External Parties	03-Dec-21	2.1	Trend Micro Security 2021 v17.0 (Consumer) contains a vulnerability that allows files inside the protected folder to be modified without any detection. **CVE ID : CVE-2021-43772**	https://helpcenter.trendmicro.com/en-us/article/tmka-10855	A-TRE-PREM-201221/440
worry-free_business_security					
Improper Privilege Management	03-Dec-21	7.2	An unnecessary privilege vulnerability in Trend Micro Worry-Free Business Security	https://success.trendmicro.com/solut	A-TRE-WORR-201221/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-44020 and 44021. **CVE ID : CVE-2021-44019**	ion/000289230	
Improper Privilege Management	03-Dec-21	7.2	An unnecessary privilege vulnerability in Trend Micro Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-44019 and 44021. **CVE ID : CVE-2021-44020**	https://success.trendmicro.com/solution/000289230	A-TRE-WORR-201221/442
Improper Privilege Management	03-Dec-21	7.2	An unnecessary privilege vulnerability in Trend Micro Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-	https://success.trendmicro.com/solution/000289230	A-TRE-WORR-201221/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-44019 and 44020. **CVE ID : CVE-2021-44021**		
Trustwave					
modsecurity					
Uncontrolled Recursion	07-Dec-21	5	ModSecurity 3.x through 3.0.5 mishandles excessively nested JSON objects. Crafted JSON objects with nesting tens-of-thousands deep could result in the web server being unable to service legitimate requests. Even a moderately large (e.g., 300KB) HTTP request can occupy one of the limited NGINX worker processes for minutes and consume almost all of the available CPU on the machine. Modsecurity 2 is similarly vulnerable: the affected versions include 2.8.0 through 2.9.4. **CVE ID : CVE-2021-42717**	https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/modsecurity-dos-vulnerability-in-json-parsing-cve-2021-42717/	A-TRU-MODS-201221/444
tsmuxer_project					
tsmuxer					
Out-of-bounds Write	03-Dec-21	7.5	tsMuxer v2.6.16 was discovered to contain a heap-based buffer overflow via the function BitStreamReader::getCurVal in bitStream.h. **CVE ID : CVE-2021-35344**	https://github.com/justdan96/tsMuxer/pull/439/commits/3a889a37b5b74a45025aca13ebda394b8f706ef3	A-TSM-TSMU-201221/445
Out-of-bounds Write	03-Dec-21	7.5	tsMuxer v2.6.16 was discovered to contain a heap-based buffer overflow via the function	https://github.com/justdan96/tsMuxer/pull/422/fil	A-TSM-TSMU-201221/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HevcSpsUnit::short_term_ref_pic_set(int) in hevc.cpp. **CVE ID : CVE-2021-35346**	es	
utils.js_project					
utils.js					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	08-Dec-21	7.5	utils.js is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') **CVE ID : CVE-2021-3815**	https://huntr.dev/bounties/20f48c63-f078-4173-bcac-a9f34885f2c0, https://github.com/fabiocaccamo/utils.js/commit/102efafb291ce1916985514440d3bf8a6826890a	A-UTI-UTIL-201221/447
Veritas					
enterprise_vault					
Deserialization of Untrusted Data	06-Dec-21	6.8	An issue (1 of 6) was discovered in Veritas Enterprise Vault through 14.1.2. On start-up, the Enterprise Vault application starts several services that listen on random .NET Remoting TCP ports for possible commands from client applications. These TCP services can be exploited due to deserialization behavior that is inherent to the .NET Remoting service. A malicious attacker can exploit both TCP remoting services and local IPC services on the	https://www.veritas.com/content/support/en_US/security/VTS21-003	A-VER-ENTE-201221/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Vault Server. This vulnerability is mitigated by properly configuring the servers and firewall as described in the vendor's security alert for this vulnerability (VTS21-003, ZDI-CAN-14078). **CVE ID : CVE-2021-44677**		
Deserialization of Untrusted Data	06-Dec-21	6.8	An issue (2 of 6) was discovered in Veritas Enterprise Vault through 14.1.2. On start-up, the Enterprise Vault application starts several services that listen on random .NET Remoting TCP ports for possible commands from client applications. These TCP services can be exploited due to deserialization behavior that is inherent to the .NET Remoting service. A malicious attacker can exploit both TCP remoting services and local IPC services on the Enterprise Vault Server. This vulnerability is mitigated by properly configuring the servers and firewall as described in the vendor's security alert for this vulnerability (VTS21-003, ZDI-CAN-14076). **CVE ID : CVE-2021-44678**	https://www.veritas.com/content/support/en_US/security/VTS21-003	A-VER-ENTE-201221/449
Deserialization of Untrusted Data	06-Dec-21	6.8	An issue (3 of 6) was discovered in Veritas Enterprise Vault through 14.1.2. On start-up, the Enterprise Vault application	https://www.veritas.com/content/support/en_US/security/V	A-VER-ENTE-201221/450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			starts several services that listen on random .NET Remoting TCP ports for possible commands from client applications. These TCP services can be exploited due to deserialization behavior that is inherent to the .NET Remoting service. A malicious attacker can exploit both TCP remoting services and local IPC services on the Enterprise Vault Server. This vulnerability is mitigated by properly configuring the servers and firewall as described in the vendor's security alert for this vulnerability (VTS21-003, ZDI-CAN-14074). **CVE ID : CVE-2021-44679**	TS21-003	
Deserialization of Untrusted Data	06-Dec-21	6.8	An issue (4 of 6) was discovered in Veritas Enterprise Vault through 14.1.2. On start-up, the Enterprise Vault application starts several services that listen on random .NET Remoting TCP ports for possible commands from client applications. These TCP services can be exploited due to deserialization behavior that is inherent to the .NET Remoting service. A malicious attacker can exploit both TCP remoting services and local IPC services on the Enterprise Vault Server. This vulnerability is mitigated by	https://www.veritas.com/content/support/en_US/security/VTS21-003	A-VER-ENTE-201221/451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properly configuring the servers and firewall as described in the vendor's security alert for this vulnerability (VTS21-003, ZDI-CAN-14075). **CVE ID : CVE-2021-44680**		
Deserialization of Untrusted Data	06-Dec-21	6.8	An issue (5 of 6) was discovered in Veritas Enterprise Vault through 14.1.2. On start-up, the Enterprise Vault application starts several services that listen on random .NET Remoting TCP ports for possible commands from client applications. These TCP services can be exploited due to deserialization behavior that is inherent to the .NET Remoting service. A malicious attacker can exploit both TCP remoting services and local IPC services on the Enterprise Vault Server. This vulnerability is mitigated by properly configuring the servers and firewall as described in the vendor's security alert for this vulnerability (VTS21-003, ZDI-CAN-14080). **CVE ID : CVE-2021-44681**	https://www.veritas.com/content/support/en_US/security/VTS21-003	A-VER-ENTE-201221/452
Deserialization of Untrusted Data	06-Dec-21	6.8	An issue (6 of 6) was discovered in Veritas Enterprise Vault through 14.1.2. On start-up, the Enterprise Vault application starts several services that listen on random .NET	https://www.veritas.com/content/support/en_US/security/VTS21-003	A-VER-ENTE-201221/453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Remoting TCP ports for possible commands from client applications. These TCP services can be exploited due to deserialization behavior that is inherent to the .NET Remoting service. A malicious attacker can exploit both TCP remoting services and local IPC services on the Enterprise Vault Server. This vulnerability is mitigated by properly configuring the servers and firewall as described in the vendor's security alert for this vulnerability (VTS21-003, ZDI-CAN-14079). **CVE ID : CVE-2021-44682**		
VIM					
vim					
Heap-based Buffer Overflow	01-Dec-21	6.8	vim is vulnerable to Heap-based Buffer Overflow **CVE ID : CVE-2021-3984**	https://github.com/vim/vim/commit/2de9b7c7c8791da8853a9a7ca9c467867465b655, https://huntr.dev/bounties/b114b5a2-18e2-49f0-b350-15994d71426a	A-VIM-VIM-201221/454
Heap-based Buffer Overflow	01-Dec-21	6.8	vim is vulnerable to Heap-based Buffer Overflow **CVE ID : CVE-2021-4019**	https://github.com/vim/vim/commit/bd228fd097	A-VIM-VIM-201221/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				b41a798f90944b5d1245eddd484142, https://huntr.dev/bounties/d8798584-a6c9-4619-b18f-001b9a6fca92	
Use After Free	06-Dec-21	6.8	vim is vulnerable to Use After Free **CVE ID : CVE-2021-4069**	https://huntr.dev/bounties/0efd6d23-2259-4081-9ff1-3ade26907d74, https://github.com/vim/vim/commit/e031fe90cf2e375ce861ff5e5e281e4ad229ebb9	A-VIM-VIM-201221/456
Wbce					
wbce_cms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Dec-21	7.5	wbce_cms is vulnerable to Improper Neutralization of Special Elements used in an SQL Command **CVE ID : CVE-2021-3817**	https://github.com/wbce/wbce_cms/commit/6ca63f0cad5f0cd606fdb69a372f09b7d238f1d7, https://huntr.dev/bounties/c330dc0d-220a-4b15-b785-	A-WBC-WBCE-201221/457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				5face4cf6ef7	
whatsapp					
whatsapp					
Out-of-bounds Write	07-Dec-21	7.5	A missing bounds check in image blurring code prior to WhatsApp for Android v2.21.22.7 and WhatsApp Business for Android v2.21.22.7 could have allowed an out-of-bounds write if a user sent a malicious image. **CVE ID : CVE-2021-24041**	https://www.whatsapp.com/security/advisories/2021/	A-WHA-WHAT-201221/458
whatsapp_business					
Out-of-bounds Write	07-Dec-21	7.5	A missing bounds check in image blurring code prior to WhatsApp for Android v2.21.22.7 and WhatsApp Business for Android v2.21.22.7 could have allowed an out-of-bounds write if a user sent a malicious image. **CVE ID : CVE-2021-24041**	https://www.whatsapp.com/security/advisories/2021/	A-WHA-WHAT-201221/459
Woocommerce					
woocommerce_currency_switcher					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-21	4.3	The WOOCS WordPress plugin before 1.3.7.1 does not sanitise and escape the key parameter of the woocs_update_profiles_data AJAX action (available to any authenticated user) before outputting it back in the response, leading to a Reflected cross-Site Scripting issue	N/A	A-WOO-WOOC-201221/460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24938		
wpdataaccess					
wp_data_access					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Dec-21	7.5	The WP Data Access WordPress plugin before 5.0.0 does not properly sanitise and escape the backup_date parameter before using it a SQL statement, leading to a SQL injection issue and could allow arbitrary table deletion **CVE ID : CVE-2021-24866**	N/A	A-WPD-WP_D-201221/461
wpserveur					
wps_hide_login					
Incorrect Authorization	06-Dec-21	5	The WPS Hide Login WordPress plugin before 1.9.1 has a bug which allows to get the secret login page by setting a random referer string and making a request to /wp-admin/options.php as an unauthenticated user. **CVE ID : CVE-2021-24917**	N/A	A-WPS-WPS_-201221/462
wp_google_fonts_project					
wp_google_fonts					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-21	4.3	The WP Google Fonts WordPress plugin before 3.1.5 does not escape the googlefont_ajax_name and googlefont_ajax_family parameter of the googlefont_action AJAx action (available to any authenticated user) before outputing them in attributes, leading Reflected Cross-Site	https://plugins.trac.wordpress.org/changeset/2623659	A-WP_-WP_G-201221/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Scripting issues **CVE ID : CVE-2021-24935**		
Wso2					
api_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-21	4.3	In accountrecoveryendpoint/recoverpassword.do in WSO2 Identity Server 5.7.0, it is possible to perform a DOM-Based XSS attack affecting the callback parameter modifying the URL that precedes the callback parameter. Once the username or password reset procedure is completed, the JavaScript code will be executed. (recoverpassword.do also has an open redirect issue for a similar reason.) **CVE ID : CVE-2021-36760**	https://docs.wso2.com/display/Security/2021+Advisories, https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1314	A-WSO-API_-201221/464
identity_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-21	4.3	In accountrecoveryendpoint/recoverpassword.do in WSO2 Identity Server 5.7.0, it is possible to perform a DOM-Based XSS attack affecting the callback parameter modifying the URL that precedes the callback parameter. Once the username or password reset procedure is completed, the JavaScript code will be executed. (recoverpassword.do also has an open redirect issue for a similar reason.)	https://docs.wso2.com/display/Security/2021+Advisories, https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1314	A-WSO-IDEN-201221/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36760		
identity_server_as_key_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-21	4.3	In accountrecoveryendpoint/recoverpassword.do in WSO2 Identity Server 5.7.0, it is possible to perform a DOM-Based XSS attack affecting the callback parameter modifying the URL that precedes the callback parameter. Once the username or password reset procedure is completed, the JavaScript code will be executed. (recoverpassword.do also has an open redirect issue for a similar reason.) **CVE ID : CVE-2021-36760**	https://docs.wso2.com/display/Security/2021+Advisories, https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1314	A-WSO-IDEN-201221/466
iot_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-21	4.3	In accountrecoveryendpoint/recoverpassword.do in WSO2 Identity Server 5.7.0, it is possible to perform a DOM-Based XSS attack affecting the callback parameter modifying the URL that precedes the callback parameter. Once the username or password reset procedure is completed, the JavaScript code will be executed. (recoverpassword.do also has an open redirect issue for a similar reason.) **CVE ID : CVE-2021-36760**	https://docs.wso2.com/display/Security/2021+Advisories, https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1314	A-WSO-IOT_-201221/467
xylem					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
aanderaa_geoview					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Dec-21	7.5	SQL injection vulnerability was discovered in Aanderaa GeoView Webservice prior to version 2.1.3 that could allow an unauthenticated attackers to execute arbitrary commands. **CVE ID : CVE-2021-41063**	https://www.xylem.com/siteassets/about-xylem/cybersecurity/advisories/xylem-aanderaa-psa-2021-003.pdf, https://www.xylem.com	A-XYL-AAND-201221/468
yejiao					
tuzicms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Dec-21	7.5	SQL Injection vulnerability exists in TuziCMS v2.0.6 in App\Manage\Controller\GuestbookController.class.php. **CVE ID : CVE-2021-44347**	N/A	A-YEJ-TUZI-201221/469
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Dec-21	7.5	SQL Injection vulnerability exists in TuziCMS v2.0.6 via the id parameer in App\Manage\Controller\AdvertController.class.php. **CVE ID : CVE-2021-44348**	N/A	A-YEJ-TUZI-201221/470
Improper Neutralization of Special Elements used in an SQL	03-Dec-21	7.5	SQL Injection vulnerability exists in TuziCMS v2.0.6 via the id parameter in App\Manage\Controller\DownloadController.class.php.	N/A	A-YEJ-TUZI-201221/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			**CVE ID : CVE-2021-44349**		
yetiforce					
yetiforce_customer_relationship_management					
Cross-Site Request Forgery (CSRF)	11-Dec-21	4.3	yetiforcecrm is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-4092**	https://hunter.dev/bounties/7b58c160-bb62-45fe-ad1f-38354378b89e, https://github.com/yetiforcecompany/yetiforcecrm/commit/585da04bb72d36a894f6ea5939ab909e53fd8c23	A-YET-YETI-201221/472
yubico					
yubihsm_2_software_development_kit					
Out-of-bounds Write	08-Dec-21	7.8	The Yubico YubiHSM YubiHSM2 library 2021.08, included in the yubihsm-shell project, does not properly validate the length of some operations including SSH signing requests, and some data operations received from a YubiHSM 2 device. **CVE ID : CVE-2021-43399**	https://www.yubico.com/support/security-advisories/ysa-2021-04/	A-YUB-YUBI-201221/473
yurunproxy_project					
yurunproxy					
Improper Neutralization of Input	01-Dec-21	4.3	YurunProxy v0.01 is affected by a Cross Site Scripting (XSS) vulnerability in	N/A	A-YUR-YURU-201221/474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			src/Client.php. The exit function will terminate the script and print a message which have values from the socket_read. **CVE ID : CVE-2021-43690**		
zerodream					
sakurapanel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-21	4.3	SakuraPanel v1.0.1.1 is affected by a Cross Site Scripting (XSS) vulnerability in /master/core/PostHandler.php. The exit function will terminate the script and print the message $data['proxy_name']. **CVE ID : CVE-2021-43681**	N/A	A-ZER-SAKU-201221/475
Zulip					
Zulip					
Insufficient Session Expiration	02-Dec-21	5	Zulip is an open source group chat application that combines real-time chat with threaded conversations. In affected versions expiration dates on the confirmation objects associated with email invitations were not enforced properly in the new account registration flow. A confirmation link takes a user to the check_prereg_key_and_redirect endpoint, before getting redirected to POST to /accounts/register/. The problem was that validation was happening in the	https://github.com/zulip/zulip/security/advisories/GHSA-wj76-pcqr-mf9f, https://github.com/zulip/zulip/commit/a014ef75a3a0ed7f24ebb157632ba58751e732c6	A-ZUL-ZULI-201221/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check_prereg_key_and_redirect part and not in /accounts/register/ - meaning that one could submit an expired confirmation key and be able to register. The issue is fixed in Zulip 4.8. There are no known workarounds and users are advised to upgrade as soon as possible. **CVE ID : CVE-2021-43791**		
zzcms					
zzcms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Dec-21	6.5	An SQL Injection vulnerability exists in zzcms 8.2, 8.3, 2020, and 2021 via the id parameter in admin/bad.php. **CVE ID : CVE-2021-40279**	N/A	A-ZZC-ZZCM-201221/477
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Dec-21	6.5	An SQL Injection vulnerablitly exits in zzcms 8.2, 8.3, 2020, and 2021 via the id parameter in admin/dl_sendmail.php. **CVE ID : CVE-2021-40280**	N/A	A-ZZC-ZZCM-201221/478
Improper Neutralization of Special Elements used in an SQL Command	09-Dec-21	6.5	An SQL Injection vulnerability exists in zzcms 8.2, 8.3, 2020, and 2021 in dl/dl_print.php when registering ordinary users. **CVE ID : CVE-2021-40281**	N/A	A-ZZC-ZZCM-201221/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Dec-21	6.5	An SQL Injection vulnerability exists in zzcms 8.2, 8.3, 2020, abd 2021 in dl/dl_download.php. when registering ordinary users. **CVE ID : CVE-2021-40282**	N/A	A-ZZC-ZZCM-201221/480
Incorrect Authorization	09-Dec-21	7.5	An Incorrect Access Control vulnerability exists in zzcms less than or equal to 2019 via admin.php. After disabling JavaScript, you can directly access the administrator console. **CVE ID : CVE-2021-43703**	N/A	A-ZZC-ZZCM-201221/481
Hardware					
anker					
eufy_homebase_2					
Out-of-bounds Write	08-Dec-21	10	An out-of-bounds write vulnerability exists in the CMD_DEVICE_GET_SERVER_LIST_REQUEST functionality of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h in function recv_server_device_response_msg_process. A specially-crafted network packet can lead to code execution. **CVE ID : CVE-2021-21950**	N/A	H-ANK-EUFY-201221/482
Out-of-bounds Write	08-Dec-21	10	An out-of-bounds write vulnerability exists in the CMD_DEVICE_GET_SERVER_LIST_REQUEST functionality of	N/A	H-ANK-EUFY-201221/483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the home_security binary of Anker Eufy Homebase 2 2.1.6.9h in function read_udp_push_config_file. A specially-crafted network packet can lead to code execution. **CVE ID : CVE-2021-21951**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	9	A command execution vulnerability exists in the wifi_country_code_update functionality of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h. A specially-crafted set of network packets can lead to arbitrary command execution. **CVE ID : CVE-2021-21954**	N/A	H-ANK-EUFY-201221/484
Improper Authentication	09-Dec-21	5	An authentication bypass vulnerability exists in the get_aes_key_info_by_packetid () function of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h. Generic network sniffing can lead to password recovery. An attacker can sniff network traffic to trigger this vulnerability. **CVE ID : CVE-2021-21955**	N/A	H-ANK-EUFY-201221/485
Auerswald					
comfortel_1400_ip					
Improper Authentication	13-Dec-21	5	Auerswald COMfortel 1400 IP and 2600 IP before 2.8G devices allow Authentication Bypass via the /about/../ substring.	N/A	H-AUE-COMF-201221/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40856		
comfortel_2600_ip					
Improper Authenticati on	13-Dec-21	5	Auerswald COMfortel 1400 IP and 2600 IP before 2.8G devices allow Authentication Bypass via the /about/../ substring. **CVE ID : CVE-2021-40856**	N/A	H-AUE-COMF-201221/487
comfortel_3600_ip					
Improper Authenticati on	13-Dec-21	5	Auerswald COMfortel 1400 IP and 2600 IP before 2.8G devices allow Authentication Bypass via the /about/../ substring. **CVE ID : CVE-2021-40856**	N/A	H-AUE-COMF-201221/488
compact_5500r					
N/A	07-Dec-21	10	Backdoors were discovered in Auerswald COMpact 5500R 7.8A and 8.0B devices, that allow attackers with access to the web based management application full administrative access to the device. **CVE ID : CVE-2021-40859**	N/A	H-AUE-COMP-201221/489
bkw					
solar-log_500					
Cleartext Storage of Sensitive Information	07-Dec-21	4	An issue was discovered in Solar-Log 500 before 2.8.2 Build 52 23.04.2013. In /export.html, email.html, and sms.html, cleartext passwords are stored. This may allow sensitive information to be read by someone with access to the device.	https://www.solar-log.com/en/support/firmware/	H-BKW-SOLA-201221/490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34544		
bosch					
access_easy_controller					
Improper Handling of Exceptional Conditions	08-Dec-21	5	An unauthenticated attacker is able to send a special HTTP request, that causes a service to crash. In case of a standalone VRM or BVMS with VRM installation this crash also opens the possibility to send further unauthenticated commands to the service. On some products the interface is only local accessible lowering the CVSS base score. For a list of modified CVSS scores, please see the official Bosch Advisory Appendix chapter Modified CVSS Scores for CVE-2021-23859 **CVE ID : CVE-2021-23859**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	H-BOS-ACCE-201221/491
videojet_decoder_7513					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-21	9	A crafted configuration packet sent by an authenticated administrative user can be used to execute arbitrary commands in system context. This issue also affects installations of the VRM, DIVAR IP, BVMS with VRM installed, the VIDEOJET decoder (VJD-7513 and VJD-8000). **CVE ID : CVE-2021-23862**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	H-BOS-VIDE-201221/492
videojet_decoder_8000					
Improper Neutralizatio	08-Dec-21	9	A crafted configuration packet sent by an	https://psirt.bosch.com/s	H-BOS-VIDE-201221/493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			authenticated administrative user can be used to execute arbitrary commands in system context. This issue also affects installations of the VRM, DIVAR IP, BVMS with VRM installed, the VIDEOJET decoder (VJD-7513 and VJD-8000). **CVE ID : CVE-2021-23862**	ecurity-advisories/bosch-sa-043434-bt.html	
Canon					
lbp223dw					
Weak Password Requirements	06-Dec-21	7.8	In Canon LBP223 printers, the System Manager Mode login does not require an account password or PIN. An attacker can remotely shut down the device after entering the background, creating a denial of service vulnerability. **CVE ID : CVE-2021-43471**	N/A	H-CAN-LBP2-201221/494
circutor					
compact_dc-s_basic					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-21	10	Buffer overflow vulnerability in function SetFirewall in index.cgi in CIRCUTOR COMPACT DC-S BASIC smart metering concentrator Firwmare version CIR_CDC_v1.2.17, allows attackers to execute arbitrary code. **CVE ID : CVE-2021-26777**	N/A	H-CIR-COMP-201221/495
Citrix					
application_delivery_controller					
Uncontrolled	07-Dec-21	4.3	A unauthenticated denial of	https://supp	H-CIT-APPL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			service vulnerability exists in Citrix ADC <13.0-83.27, <12.1-63.22 and 11.1-65.23 when configured as a VPN (Gateway) or AAA virtual server could allow an attacker to cause a temporary disruption of the Management GUI, Nitro API, and RPC communication. **CVE ID : CVE-2021-22955**	ort.citrix.com/article/CTX330728	201221/496
Uncontrolled Resource Consumption	07-Dec-21	4.3	An uncontrolled resource consumption vulnerability exists in Citrix ADC <13.0-83.27, <12.1-63.22 and 11.1-65.23 that could allow an attacker with access to NSIP or SNIP with management interface access to cause a temporary disruption of the Management GUI, Nitro API, and RPC communication. **CVE ID : CVE-2021-22956**	https://support.citrix.com/article/CTX330728	H-CIT-APPL-201221/497
Digi					
transport_dr64					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc.	https://digi.com	H-DIG-TRAN-201221/498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35978		
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/499
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/500
transport_sr44					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	https://digi.com	H-DIG-TRAN-201221/501
Insufficiently	10-Dec-21	4	An issue was discovered on	https://ww	H-DIG-TRAN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	w.digi.com/search/results?q=transport	201221/502
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/503
transport_vc74					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	https://digi.com	H-DIG-TRAN-201221/504
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may	https://www.digi.com/search/results?q=transpor	H-DIG-TRAN-201221/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	t	
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/506
transport_wr11					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	https://digi.com	H-DIG-TRAN-201221/507
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			decoding of other users' passwords. **CVE ID : CVE-2021-37187**		
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/509
Missing Encryption of Sensitive Data	10-Dec-21	5	An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session. **CVE ID : CVE-2021-37189**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/510
transport_wr11_xt					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc.	https://digi.com	H-DIG-TRAN-201221/511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35978		
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/512
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/513
Missing Encryption of Sensitive Data	10-Dec-21	5	An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session. **CVE ID : CVE-2021-37189**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/514
transport_wr21					
Improper Neutralization of Special Elements used in a	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution	https://digi.com	H-DIG-TRAN-201221/515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**		
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/516
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/517
Missing Encryption of Sensitive Data	10-Dec-21	5	An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session. **CVE ID : CVE-2021-37189**		
transport_wr31					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	https://digi.com	H-DIG-TRAN-201221/519
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/520
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Encryption of Sensitive Data	10-Dec-21	5	An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session. **CVE ID : CVE-2021-37189**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/522
transport_wr41					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	https://digi.com	H-DIG-TRAN-201221/523
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/524
Inadequate Encryption	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices	https://www.digi.com/s	H-DIG-TRAN-201221/525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Strength			through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	earch/results?q=transport	
Missing Encryption of Sensitive Data	10-Dec-21	5	An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session. **CVE ID : CVE-2021-37189**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/526
transport_wr44					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	https://digi.com	H-DIG-TRAN-201221/527
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may	https://www.digi.com/search/results?q=transpor	H-DIG-TRAN-201221/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	t	
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/529
Missing Encryption of Sensitive Data	10-Dec-21	5	An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session. **CVE ID : CVE-2021-37189**	https://www.digi.com/search/results?q=transport	H-DIG-TRAN-201221/530
Dlink					
dir-809					
Out-of-bounds Write	01-Dec-21	7.2	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_80046eb4 in /formSetPortTr. This vulnerability is triggered via	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--201221/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a crafted POST request. **CVE ID : CVE-2021-33265**		
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_8004776c in /formVirtualApp. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33266**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--201221/532
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_80034d60 in /formStaticDHCP. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33267**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--201221/533
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function sub_8003183C in /fromLogin. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33268**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--201221/534
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to	https://www.dlink.com/en/security-	H-DLI-DIR--201221/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			contain a stack buffer overflow vulnerability in the function FUN_8004776c in /formVirtualServ. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33269**	bulletin/	
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_800462c4 in /formAdvFirewall. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33270**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--201221/536
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function sub_80046EB4 in /formSetPortTr. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33271**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--201221/537
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_80040af8 in /formWlanSetup. This vulnerability is triggered via a crafted POST request.	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--201221/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-33274		
elecom					
edwrc-2533gst2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-EDWR-201221/539
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-EDWR-201221/540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-EDWR-201221/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-EDWR-201221/542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-EDWR-201221/543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-EDWR-201221/544
wrc-1167gst2					
Improper	01-Dec-21	7.7	ELECOM LAN routers (WRC-	https://ww	H-ELE-WRC--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**	w.elecom.co.jp/news/security/20211130-01/	201221/545
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/549
Incorrect	01-Dec-21	8.3	Improper access control	https://ww	H-ELE-WRC--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**	w.elecom.co.jp/news/security/20211130-01/	201221/550
wrc-1167gst2a					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors.	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20862		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/555
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-1167gst2h					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/560
Improper Neutralization of Special Elements used in an OS	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-1750gs					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authenticati on	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**	https://ww w.elecom.co.j p/news/secu rity/202111 30-01/	H-ELE-WRC--201221/565
Incorrect Authorizatio n	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior,	https://ww w.elecom.co.j p/news/secu rity/202111	H-ELE-WRC--201221/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**	30-01/	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-1750gsv					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/570
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2	https://www.elecom.co.jp/news/secu	H-ELE-WRC--201221/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**	rity/202111 30-01/	
Incorrect Authorizatio n	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware	https://ww w.elecom.co.j p/news/secu rity/202111 30-01/	H-ELE-WRC-- 201221/572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-1900gst					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/576
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-2533ghbk-i					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	3.5	Cross-site scripting vulnerability in ELECOM LAN router WRC-2533GHBK-I firmware v1.20 and prior allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20857**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/581
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	3.5	Cross-site scripting vulnerability in ELECOM LAN router WRC-2533GHBK-I firmware v1.20 and prior allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20858**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/582
wrc-2533gs2-b					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authenticati on	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/586
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-2533gs2-w					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page.	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20860		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/591
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-2533gst					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/596
Improper Authenticati on	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-2533gst2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/601
Cross-Site Request	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in	https://www.elecom.co.j	H-ELE-WRC--201221/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**	p/news/security/20211130-01/	
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors.	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20864		
wrc-2533gst2-g					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/607
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/612
wrc-2533gst2sp					
Improper Neutralization of Special	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A	https://www.elecom.co.jp/news/secu	H-ELE-WRC--201221/613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**	rity/20211130-01/	
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/617
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2	https://www.elecom.co.jp/news/secu	H-ELE-WRC--201221/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**	rity/20211130-01/	
wrc-2533gsta					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/622
Improper	01-Dec-21	7.7	OS command injection	https://ww	H-ELE-WRC--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**	w.elecom.co.jp/news/security/20211130-01/	201221/623
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRC--201221/624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrh-733gbk					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Dec-21	5.2	Buffer overflow vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20852**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRH--201221/625
Improper Neutralizatio	01-Dec-21	5.2	ELECOM LAN routers (WRH-733GBK firmware v1.02.9	https://www.elecom.co.j	H-ELE-WRH--201221/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute arbitrary OS commands via unspecified vectors. **CVE ID : CVE-2021-20853**	p/news/security/20211130-01/	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	5.2	ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute arbitrary OS commands via unspecified vectors. **CVE ID : CVE-2021-20854**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRH--201221/627
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	3.5	Cross-site scripting vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20855**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRH--201221/628
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	3.5	Cross-site scripting vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRH--201221/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20856		
wrh-733gwh					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Dec-21	5.2	Buffer overflow vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20852**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRH--201221/630
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	5.2	ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute arbitrary OS commands via unspecified vectors. **CVE ID : CVE-2021-20853**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRH--201221/631
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	5.2	ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute arbitrary OS commands via unspecified vectors. **CVE ID : CVE-2021-20854**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRH--201221/632
Improper Neutralizatio	01-Dec-21	3.5	Cross-site scripting vulnerability in ELECOM LAN	https://www.elecom.co.j	H-ELE-WRH--201221/633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20855**	p/news/security/20211130-01/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	3.5	Cross-site scripting vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20856**	https://www.elecom.co.jp/news/security/20211130-01/	H-ELE-WRH--201221/634
fatpipeinc					
ipvpn					
Unrestricted Upload of File with Dangerous Type	08-Dec-21	9.3	A vulnerability in the web management interface of FatPipe WARP, IPVPN, and MPVPN software prior to versions 10.1.2r60p92 and 10.2.2r44p1 could allow a remote, unauthenticated attacker to upload a file to any location on the filesystem. The FatPipe advisory identifier for this vulnerability is FPSA006. **CVE ID : CVE-2021-27860**	https://www.fatpipeinc.com/support/cve-list.php	H-FAT-IPVP-201221/635
mpvpn					
Unrestricted Upload of File with Dangerous	08-Dec-21	9.3	A vulnerability in the web management interface of FatPipe WARP, IPVPN, and MPVPN software prior to	https://www.fatpipeinc.com/support/cve-list.php	H-FAT-MPVP-201221/636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type			versions 10.1.2r60p92 and 10.2.2r44p1 could allow a remote, unauthenticated attacker to upload a file to any location on the filesystem. The FatPipe advisory identifier for this vulnerability is FPSA006. **CVE ID : CVE-2021-27860**		
warp					
Unrestricted Upload of File with Dangerous Type	08-Dec-21	9.3	A vulnerability in the web management interface of FatPipe WARP, IPVPN, and MPVPN software prior to versions 10.1.2r60p92 and 10.2.2r44p1 could allow a remote, unauthenticated attacker to upload a file to any location on the filesystem. The FatPipe advisory identifier for this vulnerability is FPSA006. **CVE ID : CVE-2021-27860**	https://www.fatpipeinc.com/support/cve-list.php	H-FAT-WARP-201221/637
Fortinet					
fortigate-1100e					
Out-of-bounds Write	08-Dec-21	6.8	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**	https://fortiguard.com/advisory/FG-IR-21-115	H-FOR-FORT-201221/638
fortigate-200f					
Out-of-	08-Dec-21	6.8	A heap-based buffer overflow	https://forti	H-FOR-FORT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**	guard.com/advisory/FG-IR-21-115	201221/639
fortigate-2600f					
Out-of-bounds Write	08-Dec-21	6.8	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**	https://fortiguard.com/advisory/FG-IR-21-115	H-FOR-FORT-201221/640
fortigate-3500f					
Out-of-bounds Write	08-Dec-21	6.8	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**	https://fortiguard.com/advisory/FG-IR-21-115	H-FOR-FORT-201221/641
fortigate-400e					
Out-of-bounds Write	08-Dec-21	6.8	A heap-based buffer overflow in the firmware signature verification function of	https://fortiguard.com/advisory/FG-	H-FOR-FORT-201221/642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**	IR-21-115	
fortigate-600e					
Out-of-bounds Write	08-Dec-21	6.8	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**	https://fortiguard.com/advisory/FG-IR-21-115	H-FOR-FORT-201221/643
fortigate_1800f					
Out-of-bounds Write	08-Dec-21	6.8	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**	https://fortiguard.com/advisory/FG-IR-21-115	H-FOR-FORT-201221/644
fortigate_2200e					
Out-of-bounds Write	08-Dec-21	6.8	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0	https://fortiguard.com/advisory/FG-IR-21-115	H-FOR-FORT-201221/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**		
fortigate_3300e					
Out-of-bounds Write	08-Dec-21	6.8	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**	https://fortiguard.com/advisory/FG-IR-21-115	H-FOR-FORT-201221/646
fortigate_3600e					
Out-of-bounds Write	08-Dec-21	6.8	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**	https://fortiguard.com/advisory/FG-IR-21-115	H-FOR-FORT-201221/647
fortigate_40f					
Out-of-bounds Write	08-Dec-21	6.8	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an	https://fortiguard.com/advisory/FG-IR-21-115	H-FOR-FORT-201221/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**		
fortigate_60f					
Out-of-bounds Write	08-Dec-21	6.8	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**	https://fortiguard.com/advisory/FG-IR-21-115	H-FOR-FORT-201221/649
fortigate_7121f					
Out-of-bounds Write	08-Dec-21	6.8	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**	https://fortiguard.com/advisory/FG-IR-21-115	H-FOR-FORT-201221/650
meru					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	7.2	A violation of secure design principles in Fortinet Meru AP version 8.6.1 and below, version 8.5.5 and below allows attacker to execute unauthorized code or commands via crafted cli commands. **CVE ID : CVE-2021-42759**	https://fortiguard.com/advisory/FG-IR-21-004	H-FOR-MERU-201221/651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gl-inet					
gl-ar150					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-21	4.3	GL.iNet GL-AR150 2.x before 3.x devices, configured as repeaters, allow cgi-bin/router_cgi?action=scanwifi XSS when an attacker creates an SSID with an XSS payload as the name. **CVE ID : CVE-2021-44148**	https://beaugraham.com/CVE-2021-44148-xss.html	H-GL--GL-A-201221/652
gryphonconnect					
gryphon_tower					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-21	4.3	A reflected cross-site scripting vulnerability exists in the url parameter of the /cgi-bin/luci/site_access/ page on the Gryphon Tower router's web interface. An attacker could exploit this issue by tricking a user into following a specially crafted link, granting the attacker javascript execution in the context of the victim's browser. **CVE ID : CVE-2021-20137**	N/A	H-GRY-GRYP-201221/653
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	8.3	An unauthenticated command injection vulnerability exists in multiple parameters in the Gryphon Tower router's web interface at /cgi-bin/luci/rc. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the web interface.	https://www.tenable.com/security/research/tra-2021-51	H-GRY-GRYP-201221/654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20138		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	8.3	An unauthenticated command injection vulnerability exists in the parameters of operation 3 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999. **CVE ID : CVE-2021-20139**	https://www.tenable.com/security/research/tra-2021-51	H-GRY-GRYP-201221/655
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	8.3	An unauthenticated command injection vulnerability exists in the parameters of operation 10 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999. **CVE ID : CVE-2021-20140**	https://www.tenable.com/security/research/tra-2021-51	H-GRY-GRYP-201221/656
Improper Neutralization of Special Elements used in an OS Command ('OS Command	09-Dec-21	8.3	An unauthenticated command injection vulnerability exists in the parameters of operation 32 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network	https://www.tenable.com/security/research/tra-2021-51	H-GRY-GRYP-201221/657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999. **CVE ID : CVE-2021-20141**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	8.3	An unauthenticated command injection vulnerability exists in the parameters of operation 41 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999. **CVE ID : CVE-2021-20142**	https://www.tenable.com/security/research/tra-2021-51	H-GRY-GRYP-201221/658
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	8.3	An unauthenticated command injection vulnerability exists in the parameters of operation 48 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999. **CVE ID : CVE-2021-20143**	https://www.tenable.com/security/research/tra-2021-51	H-GRY-GRYP-201221/659
Improper Neutralizatio	09-Dec-21	8.3	An unauthenticated command injection	https://www.tenable.co	H-GRY-GRYP-201221/660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			vulnerability exists in the parameters of operation 49 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999. **CVE ID : CVE-2021-20144**	m/security/research/tra-2021-51	
Improper Authentication	09-Dec-21	5	Gryphon Tower routers contain an unprotected openvpn configuration file which can grant attackers access to the Gryphon homebound VPN network which exposes the LAN interfaces of other users' devices connected to the same service. An attacker could leverage this to make configuration changes to, or otherwise attack victims' devices as though they were on an adjacent network. **CVE ID : CVE-2021-20145**	https://www.tenable.com/security/research/tra-2021-51	H-GRY-GRYP-201221/661
Insufficiently Protected Credentials	09-Dec-21	10	An unprotected ssh private key exists on the Gryphon devices which could be used to achieve root access to a server affiliated with Gryphon's development and infrastructure. At the time of discovery, the ssh key could be used to login to the development server hosted in Amazon Web Services.	https://www.tenable.com/security/research/tra-2021-51	H-GRY-GRYP-201221/662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20146		
hitachienergy					
fox615					
Weak Password Requirements	02-Dec-21	5.5	Weak Password Requirements vulnerability in Hitachi Energy FOX61x, XCM20 allows an attacker to gain unauthorized access to the Data Communication Network (DCN) routing configuration. This issue affects: Hitachi Energy FOX61x versions prior to R15A. Hitachi Energy XCM20 versions prior to R15A. **CVE ID : CVE-2021-40333**	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000062&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000069&LanguageCode=en&DocumentPartId=&Action=Launch	H-HIT-FOX6-201221/663
N/A	02-Dec-21	5	Missing Handler vulnerability in the proprietary management protocol (port TCP 5558) of Hitachi Energy FOX61x, XCM20 allows an attacker that exploits the vulnerability by activating SSH on port TCP 5558 to cause disruption to the NMS and NE communication. This issue affects: Hitachi Energy FOX61x versions prior to R15A. Hitachi Energy XCM20 versions prior to R15A.	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000062&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?Do	H-HIT-FOX6-201221/664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40334	cumentID=8DBD000069&LanguageCode=en&DocumentPartId=&Action=Launch	
xcm20					
Weak Password Requirements	02-Dec-21	5.5	Weak Password Requirements vulnerability in Hitachi Energy FOX61x, XCM20 allows an attacker to gain unauthorized access to the Data Communication Network (DCN) routing configuration. This issue affects: Hitachi Energy FOX61x versions prior to R15A. Hitachi Energy XCM20 versions prior to R15A. **CVE ID : CVE-2021-40333**	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000062&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000069&LanguageCode=en&DocumentPartId=&Action=Launch	H-HIT-XCM2-201221/665
N/A	02-Dec-21	5	Missing Handler vulnerability in the proprietary management protocol (port TCP 5558) of Hitachi Energy FOX61x, XCM20 allows an attacker that exploits the vulnerability by activating SSH on port TCP 5558 to cause disruption to the NMS and NE communication. This	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000062&LanguageCode=en&DocumentPartId=&Action=La	H-HIT-XCM2-201221/666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue affects: Hitachi Energy FOX61x versions prior to R15A. Hitachi Energy XCM20 versions prior to R15A. **CVE ID : CVE-2021-40334**	unch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000069&LanguageCode=en&DocumentPartId=&Action=Launch	
mitsubishi					
melipc_mi5122-vw					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELI-201221/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-	H-MIT-MELI-201221/668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All	019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELI-201221/669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r00_cpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r01_cpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r02_cpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r04_cpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r04_pcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r08_cpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r08_pcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20611		
melsec_iq-r_r08_sfcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20610		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r120_cpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r120_pcpu					
Uncontrolled	01-Dec-21	7.8	Uncontrolled Resource	https://ww	H-MIT-MELS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series	w.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	201221/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R	https://www.mitsubishi	H-MIT-MELS-201221/699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series	electric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r120_sfcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/1	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			00UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R	https://www.mitsubishielectric.com/	H-MIT-MELS-201221/701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series	en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r12_ccpu-v					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware	https://www.mitsubishielectric.com/en/psirt/vul	H-MIT-MELS-201221/703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions,	nerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pd	H-MIT-MELS-201221/705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All	f/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r16_cpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-	H-MIT-MELS-201221/707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All	019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r16_mtcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r16_pcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r16_sfcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r32_cpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r32_mtcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r32_pcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r32_sfcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20611		
melsec_iq-r_r64_mtcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20610		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_l02cpu\\(-p\\)					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_l06cpu\\(-p\\)					
Uncontrolled	01-Dec-21	7.8	Uncontrolled Resource	https://ww	H-MIT-MELS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series	w.mitsubishi electric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	201221/736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R	https://www.mitsubishi	H-MIT-MELS-201221/738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series	electric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_l26cpu-\\(p\\)bt					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/1	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			00UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R	https://www.mitsubishielectric.com/	H-MIT-MELS-201221/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series	en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_l26cpu\\(-p\\)					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware	https://www.mitsubishielectric.com/en/psirt/vul	H-MIT-MELS-201221/742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions,	nerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pd	H-MIT-MELS-201221/744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All	f/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_mr-mq100					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-	H-MIT-MELS-201221/746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All	019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q03udecpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q03udvcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q04udecpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q04udpvcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q04udvcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q06udecpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q06udpvcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20611		
melsec_q06udvcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20610		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q100udecpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q10udecpu					
Uncontrolled	01-Dec-21	7.8	Uncontrolled Resource	https://ww	H-MIT-MELS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series	w.mitsubishi electric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	201221/775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R	https://www.mitsubishi	H-MIT-MELS-201221/777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series	electric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q12dccpu-v					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/1	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			00UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R	https://www.mitsubishielectric.com/	H-MIT-MELS-201221/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series	en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q13udecpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware	https://www.mitsubishielectric.com/en/psirt/vul	H-MIT-MELS-201221/781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions,	nerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pd	H-MIT-MELS-201221/783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All	f/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q13udpvcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-	H-MIT-MELS-201221/785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All	019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q13udvcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q170mcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q170mscpu\\(-s1\\)					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q172dcpu-s1					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q172dscpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q173dcpu-s1					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q173dscpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20611		
melsec_q20udecpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20610		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q24dhccpu-ls					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q24dhccpu-v\\(g\\)					
Uncontrolled	01-Dec-21	7.8	Uncontrolled Resource	https://ww	H-MIT-MELS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series	w.mitsubishi electric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	201221/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R	https://www.mitsubishi	H-MIT-MELS-201221/816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series	electric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q26dhccpu-ls					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/1	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			00UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R	https://www.mitsubishielectric.com/	H-MIT-MELS-201221/818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series	en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q26udecpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware	https://www.mitsubishielectric.com/en/psirt/vul	H-MIT-MELS-201221/820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions,	nerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pd	H-MIT-MELS-201221/822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All	f/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q26udpvcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-	H-MIT-MELS-201221/824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All	019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/825

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q26udvcpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q50udecpu					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	H-MIT-MELS-201221/831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
Netgear					
rax35					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Dec-21	3.6	A path traversal attack in web interfaces of Netgear RAX35, RAX38, and RAX40 routers before v1.0.4.102, allows a remote unauthenticated attacker to gain access to sensitive restricted information, such as forbidden files of the web	http://netgear.com, https://kb.netgear.com/000064405/Security-Advisory-for-Path-Traversal-	H-NET-RAX3-201221/832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application, via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41449**	on-Some-Routers-PSV-2021-0268, https://www.netgear.com/about/security/	
rax38					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Dec-21	3.6	A path traversal attack in web interfaces of Netgear RAX35, RAX38, and RAX40 routers before v1.0.4.102, allows a remote unauthenticated attacker to gain access to sensitive restricted information, such as forbidden files of the web application, via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41449**	http://netgear.com, https://kb.netgear.com/000064405/Security-Advisory-for-Path-Traversal-on-Some-Routers-PSV-2021-0268, https://www.netgear.com/about/security/	H-NET-RAX3-201221/833
rax40					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Dec-21	3.6	A path traversal attack in web interfaces of Netgear RAX35, RAX38, and RAX40 routers before v1.0.4.102, allows a remote unauthenticated attacker to gain access to sensitive restricted information, such as forbidden files of the web application, via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41449**	http://netgear.com, https://kb.netgear.com/000064405/Security-Advisory-for-Path-Traversal-on-Some-Routers-PSV-2021-0268, https://www.netgear.com/about/sec	H-NET-RAX4-201221/834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				urity/	
Nttdocomo					
wi-fi_station_sh-52a					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	4.3	Cross-site scripting vulnerability in Wi-Fi STATION SH-52A (38JP_1_11G, 38JP_1_11J, 38JP_1_11K, 38JP_1_11L, 38JP_1_26F, 38JP_1_26G, 38JP_1_26J, 38JP_2_03B, and 38JP_2_03C) allows a remote unauthenticated attacker to inject an arbitrary script via WebUI of the device. **CVE ID : CVE-2021-20847**	N/A	H-NTT-WI-F-201221/835
nxp					
i.mx6sx					
Incorrect Permission Assignment for Critical Resource	07-Dec-21	3.6	The OPTEE-OS CSU driver for NXP i.MX SoC devices lacks security access configuration for several models, resulting in TrustZone bypass because the NonSecure World can perform arbitrary memory read/write operations on Secure World memory. This involves a DMA capable peripheral. **CVE ID : CVE-2021-36133**	N/A	H-NXP-I.MX-201221/836
i.mx_6					
Incorrect Permission Assignment for Critical Resource	07-Dec-21	3.6	The OPTEE-OS CSU driver for NXP i.MX SoC devices lacks security access configuration for several models, resulting in TrustZone bypass because the NonSecure World can perform arbitrary memory read/write operations on	N/A	H-NXP-I.MX-201221/837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Secure World memory. This involves a DMA capable peripheral. **CVE ID : CVE-2021-36133**		
i.mx_6solox					
Incorrect Permission Assignment for Critical Resource	07-Dec-21	3.6	The OPTEE-OS CSU driver for NXP i.MX SoC devices lacks security access configuration for several models, resulting in TrustZone bypass because the NonSecure World can perform arbitrary memory read/write operations on Secure World memory. This involves a DMA capable peripheral. **CVE ID : CVE-2021-36133**	N/A	H-NXP-I.MX-201221/838
i.mx_6ull					
Incorrect Permission Assignment for Critical Resource	07-Dec-21	3.6	The OPTEE-OS CSU driver for NXP i.MX SoC devices lacks security access configuration for several models, resulting in TrustZone bypass because the NonSecure World can perform arbitrary memory read/write operations on Secure World memory. This involves a DMA capable peripheral. **CVE ID : CVE-2021-36133**	N/A	H-NXP-I.MX-201221/839
i.mx_6ultralite					
Incorrect Authorizatio n	07-Dec-21	4.6	An issue was discovered in Trusted Firmware OP-TEE Trusted OS through 3.15.0. The OPTEE-OS CSU driver for NXP i.MX6UL SoC devices lacks security access configuration for wakeup-	https://github.com/f-secure-foundry/advisories/blob/master/Security_Advisory	H-NXP-I.MX-201221/840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			related registers, resulting in TrustZone bypass because the NonSecure World can perform arbitrary memory read/write operations on Secure World memory. This involves a v cycle. **CVE ID : CVE-2021-44149**	-Ref_FSC-HWSEC-VR2021-0002-OP-TEE_TrustZone_bypass_at_wakeup.txt	
i.mx_6ulz					
Incorrect Permission Assignment for Critical Resource	07-Dec-21	3.6	The OPTEE-OS CSU driver for NXP i.MX SoC devices lacks security access configuration for several models, resulting in TrustZone bypass because the NonSecure World can perform arbitrary memory read/write operations on Secure World memory. This involves a DMA capable peripheral. **CVE ID : CVE-2021-36133**	N/A	H-NXP-I.MX-201221/841
i.mx_7ds					
Incorrect Permission Assignment for Critical Resource	07-Dec-21	3.6	The OPTEE-OS CSU driver for NXP i.MX SoC devices lacks security access configuration for several models, resulting in TrustZone bypass because the NonSecure World can perform arbitrary memory read/write operations on Secure World memory. This involves a DMA capable peripheral. **CVE ID : CVE-2021-36133**	N/A	H-NXP-I.MX-201221/842
kinetis_k82					
Out-of-bounds Read	01-Dec-21	2.1	NXP Kinetis K82 devices have a buffer over-read via a crafted wlength value in a	N/A	H-NXP-KINE-201221/843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GET Status-Other request during use of USB In-System Programming (ISP) mode. This discloses protected flash memory. **CVE ID : CVE-2021-44479**		
lpc55s69					
Out-of-bounds Read	01-Dec-21	2.1	NXP Kinetis K82 devices have a buffer over-read via a crafted wlength value in a GET Status-Other request during use of USB In-System Programming (ISP) mode. This discloses protected flash memory. **CVE ID : CVE-2021-44479**	N/A	H-NXP-LPC5-201221/844
lpc55s69jbd100					
Out-of-bounds Read	01-Dec-21	2.1	NXP LPC55S69 devices before A3 have a buffer over-read via a crafted wlength value in a GET Descriptor Configuration request during use of USB In-System Programming (ISP) mode. This discloses protected flash memory. **CVE ID : CVE-2021-40154**	N/A	H-NXP-LPC5-201221/845
lpc55s69jbd64					
Out-of-bounds Read	01-Dec-21	2.1	NXP LPC55S69 devices before A3 have a buffer over-read via a crafted wlength value in a GET Descriptor Configuration request during use of USB In-System Programming (ISP) mode. This discloses protected flash memory. **CVE ID : CVE-2021-40154**	N/A	H-NXP-LPC5-201221/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
lpc55s69jev98					
Out-of-bounds Read	01-Dec-21	2.1	NXP LPC55S69 devices before A3 have a buffer over-read via a crafted wlength value in a GET Descriptor Configuration request during use of USB In-System Programming (ISP) mode. This discloses protected flash memory. **CVE ID : CVE-2021-40154**	N/A	H-NXP-LPC5-201221/847
renesas					
rx65					
Insufficiently Protected Credentials	02-Dec-21	2.1	An issue was discovered on Renesas RX65 and RX65N devices. With a VCC glitch, an attacker can extract the security ID key from the device. Then, the protected firmware can be extracted. **CVE ID : CVE-2021-43327**	N/A	H-REN-RX65-201221/848
rx65n					
Insufficiently Protected Credentials	02-Dec-21	2.1	An issue was discovered on Renesas RX65 and RX65N devices. With a VCC glitch, an attacker can extract the security ID key from the device. Then, the protected firmware can be extracted. **CVE ID : CVE-2021-43327**	N/A	H-REN-RX65-201221/849
solardatasystems					
solar-log_500					
Missing Authorization	07-Dec-21	5	The web administration server in Solar-Log 500 before 2.8.2 Build 52 does not require authentication, which allows remote attackers to	https://www.solar-log.com/en/support/firmware/	H-SOL-SOLA-201221/850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			gain administrative privileges by connecting to the server. As a result, the attacker can modify configuration files and change the system status. **CVE ID : CVE-2021-34543**		
Sonicwall					
sma_200					
Out-of-bounds Write	08-Dec-21	7.5	A Stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod_cgi module environment variables allows a remote unauthenticated attacker to potentially execute code as a 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions. **CVE ID : CVE-2021-20038**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/851
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	Improper neutralization of special elements in the SMA100 management interface '/cgi-bin/viewcert' POST http method allows a remote authenticated attacker to inject arbitrary commands as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20039**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/852
Improper Limitation of a Pathname	08-Dec-21	5	A relative path traversal vulnerability in the SMA100 upload funtion allows a	https://psirt.global.sonicwall.com/vul	H-SON-SMA_-201221/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			remote unauthenticated attacker to upload crafted web pages or files as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20040**	n-detail/SNWLID-2021-0026	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Dec-21	7.8	An unauthenticated and remote adversary can consume all of the device's CPU due to crafted HTTP requests sent to SMA100 /fileshare/sonicfiles/sonicfiles resulting in a loop with unreachable exit condition. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20041**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/854
Externally Controlled Reference to a Resource in Another Sphere	08-Dec-21	7.5	An unauthenticated remote attacker can use SMA 100 as an unintended proxy or intermediary undetectable proxy to bypass firewall rules. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20042**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/855
Out-of-bounds Write	08-Dec-21	6.5	A Heap-based buffer overflow vulnerability in SonicWall SMA100 getBookmarks method allows a remote authenticated attacker to potentially execute code as the nobody user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20043		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	A post-authentication remote command injection vulnerability in SonicWall SMA100 allows a remote authenticated attacker to execute OS system commands in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20044**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/857
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	7.5	A buffer overflow vulnerability in SMA100 sonicfiles RAC_COPY_TO (RacNumber 36) method allows a remote unauthenticated attacker to potentially execute code as the 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20045**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/858
sma_210					
Out-of-bounds Write	08-Dec-21	7.5	A Stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod_cgi module environment variables allows a remote unauthenticated attacker to potentially execute code as a 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20038		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	Improper neutralization of special elements in the SMA100 management interface '/cgi-bin/viewcert' POST http method allows a remote authenticated attacker to inject arbitrary commands as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20039**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/860
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-21	5	A relative path traversal vulnerability in the SMA100 upload funtion allows a remote unauthenticated attacker to upload crafted web pages or files as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20040**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/861
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Dec-21	7.8	An unauthenticated and remote adversary can consume all of the device's CPU due to crafted HTTP requests sent to SMA100 /fileshare/sonicfiles/sonicfiles resulting in a loop with unreachable exit condition. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20041**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/862
Externally Controlled Reference to	08-Dec-21	7.5	An unauthenticated remote attacker can use SMA 100 as an unintended proxy or	https://psirt.global.sonicwall.com/vul	H-SON-SMA_-201221/863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Resource in Another Sphere			intermediary undetectable proxy to bypass firewall rules. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20042**	n-detail/SNWLID-2021-0026	
Out-of-bounds Write	08-Dec-21	6.5	A Heap-based buffer overflow vulnerability in SonicWall SMA100 getBookmarks method allows a remote authenticated attacker to potentially execute code as the nobody user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20043**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/864
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	A post-authentication remote command injection vulnerability in SonicWall SMA100 allows a remote authenticated attacker to execute OS system commands in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20044**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/865
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	7.5	A buffer overflow vulnerability in SMA100 sonicfiles RAC_COPY_TO (RacNumber 36) method allows a remote unauthenticated attacker to potentially execute code as the 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20045		
sma_400					
Out-of-bounds Write	08-Dec-21	7.5	A Stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod_cgi module environment variables allows a remote unauthenticated attacker to potentially execute code as a 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions. **CVE ID : CVE-2021-20038**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/867
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	Improper neutralization of special elements in the SMA100 management interface '/cgi-bin/viewcert' POST http method allows a remote authenticated attacker to inject arbitrary commands as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20039**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/868
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-21	5	A relative path traversal vulnerability in the SMA100 upload funtion allows a remote unauthenticated attacker to upload crafted web pages or files as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20040		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Dec-21	7.8	An unauthenticated and remote adversary can consume all of the device's CPU due to crafted HTTP requests sent to SMA100 /fileshare/sonicfiles/sonicfiles resulting in a loop with unreachable exit condition. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20041**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/870
Externally Controlled Reference to a Resource in Another Sphere	08-Dec-21	7.5	An unauthenticated remote attacker can use SMA 100 as an unintended proxy or intermediary undetectable proxy to bypass firewall rules. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20042**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/871
Out-of-bounds Write	08-Dec-21	6.5	A Heap-based buffer overflow vulnerability in SonicWall SMA100 getBookmarks method allows a remote authenticated attacker to potentially execute code as the nobody user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20043**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/872
Improper Neutralization of Special Elements used in an OS Command	08-Dec-21	9	A post-authentication remote command injection vulnerability in SonicWall SMA100 allows a remote authenticated attacker to execute OS system commands	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-	H-SON-SMA_-201221/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20044**	0026	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	7.5	A buffer overflow vulnerability in SMA100 sonicfiles RAC_COPY_TO (RacNumber 36) method allows a remote unauthenticated attacker to potentially execute code as the 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20045**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/874
sma_410					
Out-of-bounds Write	08-Dec-21	7.5	A Stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod_cgi module environment variables allows a remote unauthenticated attacker to potentially execute code as a 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions. **CVE ID : CVE-2021-20038**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/875
Improper Neutralization of Special Elements used in an OS Command	08-Dec-21	9	Improper neutralization of special elements in the SMA100 management interface '/cgi-bin/viewcert' POST http method allows a remote authenticated	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-	H-SON-SMA_-201221/876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			attacker to inject arbitrary commands as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20039**	0026	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-21	5	A relative path traversal vulnerability in the SMA100 upload funtion allows a remote unauthenticated attacker to upload crafted web pages or files as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20040**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/877
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Dec-21	7.8	An unauthenticated and remote adversary can consume all of the device's CPU due to crafted HTTP requests sent to SMA100 /fileshare/sonicfiles/sonicfiles resulting in a loop with unreachable exit condition. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20041**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/878
Externally Controlled Reference to a Resource in Another Sphere	08-Dec-21	7.5	An unauthenticated remote attacker can use SMA 100 as an unintended proxy or intermediary undetectable proxy to bypass firewall rules. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20042**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Dec-21	6.5	A Heap-based buffer overflow vulnerability in SonicWall SMA100 getBookmarks method allows a remote authenticated attacker to potentially execute code as the nobody user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20043**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/880
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	A post-authentication remote command injection vulnerability in SonicWall SMA100 allows a remote authenticated attacker to execute OS system commands in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20044**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/881
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	7.5	A buffer overflow vulnerability in SMA100 sonicfiles RAC_COPY_TO (RacNumber 36) method allows a remote unauthenticated attacker to potentially execute code as the 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20045**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/882
sma_500v					
Out-of-bounds Write	08-Dec-21	7.5	A Stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod_cgi module	https://psirt.global.sonicwall.com/vuln-	H-SON-SMA_-201221/883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			environment variables allows a remote unauthenticated attacker to potentially execute code as a 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions. **CVE ID : CVE-2021-20038**	detail/SNWLID-2021-0026	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	Improper neutralization of special elements in the SMA100 management interface '/cgi-bin/viewcert' POST http method allows a remote authenticated attacker to inject arbitrary commands as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20039**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/884
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-21	5	A relative path traversal vulnerability in the SMA100 upload funtion allows a remote unauthenticated attacker to upload crafted web pages or files as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20040**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/885
Loop with Unreachable Exit Condition ('Infinite	08-Dec-21	7.8	An unauthenticated and remote adversary can consume all of the device's CPU due to crafted HTTP requests sent to SMA100	https://psirt.global.sonicwall.com/vuln-detail/SNWL	H-SON-SMA_-201221/886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop')			/fileshare/sonicfiles/sonicfiles resulting in a loop with unreachable exit condition. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20041**	ID-2021-0026	
Externally Controlled Reference to a Resource in Another Sphere	08-Dec-21	7.5	An unauthenticated remote attacker can use SMA 100 as an unintended proxy or intermediary undetectable proxy to bypass firewall rules. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20042**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/887
Out-of-bounds Write	08-Dec-21	6.5	A Heap-based buffer overflow vulnerability in SonicWall SMA100 getBookmarks method allows a remote authenticated attacker to potentially execute code as the nobody user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20043**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/888
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	A post-authentication remote command injection vulnerability in SonicWall SMA100 allows a remote authenticated attacker to execute OS system commands in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20044**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	7.5	A buffer overflow vulnerability in SMA100 sonicfiles RAC_COPY_TO (RacNumber 36) method allows a remote unauthenticated attacker to potentially execute code as the 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20045**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	H-SON-SMA_-201221/890
Tendacn					
ac15					
Out-of-bounds Write	03-Dec-21	7.5	A Stack-based Buffer Overflow vulnerability exists in the Tenda AC15 V15.03.05.18_multi device via the list parameter in a post request in goform/SetIpMacBind. **CVE ID : CVE-2021-44352**	N/A	H-TEN-AC15-201221/891
Tp-link					
archer_ax10					
Exposure of Resource to Wrong Sphere	07-Dec-21	7.8	A denial-of-service attack in WPA2, and WPA3-SAE authentication methods in TP-Link AX10v1 before V1_211014, allows a remote unauthenticated attacker to disconnect an already connected wireless client via sending with a wireless adapter specific spoofed authentication frames **CVE ID : CVE-2021-40288**	https://www.tp-link.com/us/support/download/archer-ax10/v1/#Firmware	H-TP--ARCH-201221/892
archer_ax10_v1					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	08-Dec-21	5	An HTTP request smuggling attack in TP-Link AX10v1 before v1_211117 allows a remote unauthenticated attacker to DoS the web application via sending a specific HTTP packet. **CVE ID : CVE-2021-41450**	https://www.tp-link.com/us/support/download/archer-ax10/v1/#Firmware, http://tp-link.com	H-TP--ARCH-201221/893
vinga					
wr-n300u					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Dec-21	6.5	VINGA WR-N300U 77.102.1.4853 is affected by a command execution vulnerability in the goahead component. **CVE ID : CVE-2021-43469**	N/A	H-VIN-WR-N-201221/894
webhmi					
webhmi					
Improper Authentication	06-Dec-21	7.5	The authentication algorithm of the WebHMI portal is sound, but the implemented mechanism can be bypassed as the result of a separate weakness that is primary to the authentication error. **CVE ID : CVE-2021-43931**	https://us-cert.cisa.gov/ics/advisories/icsa-21-336-03	H-WEB-WEBH-201221/895
Unrestricted Upload of File with Dangerous Type	06-Dec-21	10	The software allows the attacker to upload or transfer files of dangerous types to the WebHMI portal, that may be automatically processed within the product's environment or lead to arbitrary code execution.	https://us-cert.cisa.gov/ics/advisories/icsa-21-336-03	H-WEB-WEBH-201221/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-43936		
wokkalokka					
wokka_watch_q50					
Missing Encryption of Sensitive Data	01-Dec-21	9.3	Wokka Lokka Q50 devices through 2021-11-30 allow remote attackers (who know the SIM phone number and password) to listen to a device's surroundings via a callback in an SMS command, as demonstrated by the 123456 and 523681 default passwords. **CVE ID : CVE-2021-44480**	N/A	H-WOK-WOKK-201221/897
Operating System					
anker					
eufy_homebase_2_firmware					
Out-of-bounds Write	08-Dec-21	10	An out-of-bounds write vulnerability exists in the CMD_DEVICE_GET_SERVER_LIST_REQUEST functionality of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h in function recv_server_device_response_msg_process. A specially-crafted network packet can lead to code execution. **CVE ID : CVE-2021-21950**	N/A	O-ANK-EUFY-201221/898
Out-of-bounds Write	08-Dec-21	10	An out-of-bounds write vulnerability exists in the CMD_DEVICE_GET_SERVER_LIST_REQUEST functionality of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h in function read_udp_push_config_file. A specially-crafted network	N/A	O-ANK-EUFY-201221/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packet can lead to code execution. **CVE ID : CVE-2021-21951**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	9	A command execution vulnerability exists in the wifi_country_code_update functionality of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h. A specially-crafted set of network packets can lead to arbitrary command execution. **CVE ID : CVE-2021-21954**	N/A	O-ANK-EUFY-201221/900
Improper Authentication	09-Dec-21	5	An authentication bypass vulnerability exists in the get_aes_key_info_by_packetid () function of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h. Generic network sniffing can lead to password recovery. An attacker can sniff network traffic to trigger this vulnerability. **CVE ID : CVE-2021-21955**	N/A	O-ANK-EUFY-201221/901
Apple					
macos					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-21	6.8	The executable file warning was not presented when downloading .inetloc files, which, due to a flaw in Mac OS, can run commands on a user's computer.*Note: This issue only affected Mac OS operating systems. Other operating systems are unaffected.*. This	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/,	O-APP-MACO-201221/902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38510**	https://www.mozilla.org/security/advisories/mfsa2021-48/, https://bugzilla.mozilla.org/show_bug.cgi?id=1731779	
Auerswald					
comfortel_1400_ip_firmware					
Improper Authentication	13-Dec-21	5	Auerswald COMfortel 1400 IP and 2600 IP before 2.8G devices allow Authentication Bypass via the /about/../ substring. **CVE ID : CVE-2021-40856**	N/A	O-AUE-COMF-201221/903
comfortel_2600_ip_firmware					
Improper Authentication	13-Dec-21	5	Auerswald COMfortel 1400 IP and 2600 IP before 2.8G devices allow Authentication Bypass via the /about/../ substring. **CVE ID : CVE-2021-40856**	N/A	O-AUE-COMF-201221/904
comfortel_3600_ip_firmware					
Improper Authentication	13-Dec-21	5	Auerswald COMfortel 1400 IP and 2600 IP before 2.8G devices allow Authentication Bypass via the /about/../ substring. **CVE ID : CVE-2021-40856**	N/A	O-AUE-COMF-201221/905
compact_5500r_firmware					
N/A	07-Dec-21	10	Backdoors were discovered in Auerswald COMpact 5500R 7.8A and 8.0B devices, that allow attackers with access to	N/A	O-AUE-COMP-201221/906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the web based management application full administrative access to the device. **CVE ID : CVE-2021-40859**		
bkw					
solar-log_500_firmware					
Cleartext Storage of Sensitive Information	07-Dec-21	4	An issue was discovered in Solar-Log 500 before 2.8.2 Build 52 23.04.2013. In /export.html, email.html, and sms.html, cleartext passwords are stored. This may allow sensitive information to be read by someone with access to the device. **CVE ID : CVE-2021-34544**	https://www.solar-log.com/en/support/firmware/	O-BKW-SOLA-201221/907
bosch					
access_easy_controller_firmware					
Improper Handling of Exceptional Conditions	08-Dec-21	5	An unauthenticated attacker is able to send a special HTTP request, that causes a service to crash. In case of a standalone VRM or BVMS with VRM installation this crash also opens the possibility to send further unauthenticated commands to the service. On some products the interface is only local accessible lowering the CVSS base score. For a list of modified CVSS scores, please see the official Bosch Advisory Appendix chapter Modified CVSS Scores for CVE-2021-23859	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	O-BOS-ACCE-201221/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-23859		
divar_ip_5000_firmware					
Improper Handling of Exceptional Conditions	08-Dec-21	5	An unauthenticated attacker is able to send a special HTTP request, that causes a service to crash. In case of a standalone VRM or BVMS with VRM installation this crash also opens the possibility to send further unauthenticated commands to the service. On some products the interface is only local accessible lowering the CVSS base score. For a list of modified CVSS scores, please see the official Bosch Advisory Appendix chapter Modified CVSS Scores for CVE-2021-23859 **CVE ID : CVE-2021-23859**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	O-BOS-DIVA-201221/909
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	An error in a page handler of the VRM may lead to a reflected cross site scripting (XSS) in the web-based interface. To exploit this vulnerability an attack must be able to modify the HTTP header that is sent. This issue also affects installations of the DIVAR IP and BVMS with VRM installed. **CVE ID : CVE-2021-23860**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	O-BOS-DIVA-201221/910
Improper Neutralization of Special Elements used in a Command	08-Dec-21	5.5	By executing a special command, an user with administrative rights can get access to extended debug functionality on the VRM allowing an impact on	https://psirt.bosch.com/security-advisories/bosch-sa-043434-	O-BOS-DIVA-201221/911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			integrity or availability of the installed software. This issue also affects installations of the DIVAR IP and BVMS with VRM installed. **CVE ID : CVE-2021-23861**	bt.html	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-21	9	A crafted configuration packet sent by an authenticated administrative user can be used to execute arbitrary commands in system context. This issue also affects installations of the VRM, DIVAR IP, BVMS with VRM installed, the VIDEOJET decoder (VJD-7513 and VJD-8000). **CVE ID : CVE-2021-23862**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	O-BOS-DIVA-201221/912
divar_ip_7000_firmware					
Improper Handling of Exceptional Conditions	08-Dec-21	5	An unauthenticated attacker is able to send a special HTTP request, that causes a service to crash. In case of a standalone VRM or BVMS with VRM installation this crash also opens the possibility to send further unauthenticated commands to the service. On some products the interface is only local accessible lowering the CVSS base score. For a list of modified CVSS scores, please see the official Bosch Advisory Appendix chapter Modified CVSS Scores for CVE-2021-23859 **CVE ID : CVE-2021-23859**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	O-BOS-DIVA-201221/913
Improper	08-Dec-21	4.3	An error in a page handler of	https://psirt.	O-BOS-DIVA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			the VRM may lead to a reflected cross site scripting (XSS) in the web-based interface. To exploit this vulnerability an attack must be able to modify the HTTP header that is sent. This issue also affects installations of the DIVAR IP and BVMS with VRM installed. **CVE ID : CVE-2021-23860**	bosch.com/security-advisories/bosch-sa-043434-bt.html	201221/914
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-21	5.5	By executing a special command, an user with administrative rights can get access to extended debug functionality on the VRM allowing an impact on integrity or availability of the installed software. This issue also affects installations of the DIVAR IP and BVMS with VRM installed. **CVE ID : CVE-2021-23861**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	O-BOS-DIVA-201221/915
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-21	9	A crafted configuration packet sent by an authenticated administrative user can be used to execute arbitrary commands in system context. This issue also affects installations of the VRM, DIVAR IP, BVMS with VRM installed, the VIDEOJET decoder (VJD-7513 and VJD-8000). **CVE ID : CVE-2021-23862**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	O-BOS-DIVA-201221/916
videojet_decoder_7513_firmware					
Improper Neutralization of Special	08-Dec-21	9	A crafted configuration packet sent by an authenticated administrative	https://psirt.bosch.com/security-	O-BOS-VIDE-201221/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			user can be used to execute arbitrary commands in system context. This issue also affects installations of the VRM, DIVAR IP, BVMS with VRM installed, the VIDEOJET decoder (VJD-7513 and VJD-8000). **CVE ID : CVE-2021-23862**	advisories/bosch-sa-043434-bt.html	
videojet_decoder_8000_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-21	9	A crafted configuration packet sent by an authenticated administrative user can be used to execute arbitrary commands in system context. This issue also affects installations of the VRM, DIVAR IP, BVMS with VRM installed, the VIDEOJET decoder (VJD-7513 and VJD-8000). **CVE ID : CVE-2021-23862**	https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html	O-BOS-VIDE-201221/918
Canon					
lbp223dw_firmware					
Weak Password Requirements	06-Dec-21	7.8	In Canon LBP223 printers, the System Manager Mode login does not require an account password or PIN. An attacker can remotely shut down the device after entering the background, creating a denial of service vulnerability. **CVE ID : CVE-2021-43471**	N/A	O-CAN-LBP2-201221/919
Canonical					
ubuntu_linux					
Improper	08-Dec-21	7.5	In Django 2.2 before 2.2.25,	https://docs.	O-CAN-UBUN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			3.1 before 3.1.14, and 3.2 before 3.2.10, HTTP requests for URLs with trailing newlines could bypass upstream access control based on URL paths. **CVE ID : CVE-2021-44420**	djangoproject.com/en/3.2/releases/security/, https://www.openwall.com/lists/oss-security/2021/12/07/1, https://www.djangoproject.com/weblog/2021/dec/07/security-releases/	201221/920
circutor					
compact_dc-s_basic_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-21	10	Buffer overflow vulnerability in function SetFirewall in index.cgi in CIRCUTOR COMPACT DC-S BASIC smart metering concentrator Firwmare version CIR_CDC_v1.2.17, allows attackers to execute arbitrary code. **CVE ID : CVE-2021-26777**	N/A	O-CIR-COMP-201221/921
Citrix					
application_delivery_controller_firmware					
Uncontrolled Resource Consumption	07-Dec-21	4.3	A unauthenticated denial of service vulnerability exists in Citrix ADC <13.0-83.27, <12.1-63.22 and 11.1-65.23 when configured as a VPN (Gateway) or AAA virtual server could allow an attacker to cause a temporary disruption of the	https://support.citrix.com/article/CTX330728	O-CIT-APPL-201221/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Management GUI, Nitro API, and RPC communication. **CVE ID : CVE-2021-22955**		
Uncontrolled Resource Consumption	07-Dec-21	4.3	An uncontrolled resource consumption vulnerability exists in Citrix ADC <13.0-83.27, <12.1-63.22 and 11.1-65.23 that could allow an attacker with access to NSIP or SNIP with management interface access to cause a temporary disruption of the Management GUI, Nitro API, and RPC communication. **CVE ID : CVE-2021-22956**	https://support.citrix.com/article/CTX330728	O-CIT-APPL-201221/923
Debian					
debian_linux					
Integer Overflow or Wraparound	06-Dec-21	6	runc is a CLI tool for spawning and running containers on Linux according to the OCI specification. In runc, netlink is used internally as a serialization system for specifying the relevant container configuration to the `C` portion of the code (responsible for the based namespace setup of containers). In all versions of runc prior to 1.0.3, the encoder did not handle the possibility of an integer overflow in the 16-bit length field for the byte array attribute type, meaning that a large enough malicious byte array attribute could result in the length overflowing and	https://github.com/opencontainers/runc/commit/d72d057ba794164c3cce9451a00b72a78b25e1ae, https://github.com/opencontainers/runc/commit/9c444070ec7bb83995dbc0185da68284da71c554, https://github.com/opencontainers/runc/security/advisories/GHSA-v95c-	O-DEB-DEBI-201221/924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attribute contents being parsed as netlink messages for container configuration. This vulnerability requires the attacker to have some control over the configuration of the container and would allow the attacker to bypass the namespace restrictions of the container by simply adding their own netlink payload which disables all namespaces. The main users impacted are those who allow untrusted images with untrusted configurations to run on their machines (such as with shared cloud infrastructure). runc version 1.0.3 contains a fix for this bug. As a workaround, one may try disallowing untrusted namespace paths from your container. It should be noted that untrusted namespace paths would allow the attacker to disable namespace protections entirely even in the absence of this bug. **CVE ID : CVE-2021-43784**	p5hm-xq8f	
Improper Authenticati on	08-Dec-21	7.5	In Django 2.2 before 2.2.25, 3.1 before 3.1.14, and 3.2 before 3.2.10, HTTP requests for URLs with trailing newlines could bypass upstream access control based on URL paths. **CVE ID : CVE-2021-44420**	https://docs.djangoproject.com/en/3.2/releases/security/, https://www.openwall.com/lists/oss	O-DEB-DEBI-201221/925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				-security/2021/12/07/1, https://www.djangoproject.com/weblog/2021/dec/07/security-releases/	
Digi					
transport_dr64_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	https://digi.com	O-DIG-TRAN-201221/926
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/927
Inadequate Encryption	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An	https://www.digi.com/search/result	O-DIG-TRAN-201221/928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Strength			authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	s?q=transport	
transport_sr44_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	https://digi.com	O-DIG-TRAN-201221/929
transport_vc74_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	https://digi.com	O-DIG-TRAN-201221/930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/931
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/932
transport_wr11_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	https://digi.com	O-DIG-TRAN-201221/933
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An	https://www.digi.com/search/result	O-DIG-TRAN-201221/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	s?q=transport	
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/935
Missing Encryption of Sensitive Data	10-Dec-21	5	An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session. **CVE ID : CVE-2021-37189**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/936
transport_wr11_xt_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including	https://digi.com	O-DIG-TRAN-201221/937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**		
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/938
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/939
Missing Encryption of Sensitive Data	10-Dec-21	5	An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session. **CVE ID : CVE-2021-37189**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/940
transport_wr21_firmware					
Improper	10-Dec-21	10	An issue was discovered in	https://digi.c	O-DIG-TRAN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	om	201221/941
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/942
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/943
Missing Encryption of Sensitive Data	10-Dec-21	5	An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session. **CVE ID : CVE-2021-37189**		
transport_wr31_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	https://digi.com	O-DIG-TRAN-201221/945
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/946
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic),	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			changing the behavior of the gateway. **CVE ID : CVE-2021-37188**		
Missing Encryption of Sensitive Data	10-Dec-21	5	An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session. **CVE ID : CVE-2021-37189**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/948
transport_wr41_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	https://digi.com	O-DIG-TRAN-201221/949
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords.	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-37187		
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/951
Missing Encryption of Sensitive Data	10-Dec-21	5	An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session. **CVE ID : CVE-2021-37189**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/952
transport_wr44_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Dec-21	10	An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc. **CVE ID : CVE-2021-35978**	https://digi.com	O-DIG-TRAN-201221/953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	10-Dec-21	4	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords. **CVE ID : CVE-2021-37187**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/954
Inadequate Encryption Strength	10-Dec-21	6.5	An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway. **CVE ID : CVE-2021-37188**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/955
Missing Encryption of Sensitive Data	10-Dec-21	5	An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session. **CVE ID : CVE-2021-37189**	https://www.digi.com/search/results?q=transport	O-DIG-TRAN-201221/956
Dlink					
dir-809_firmware					
Out-of-bounds Write	01-Dec-21	7.2	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--201221/957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow vulnerability in the function FUN_80046eb4 in /formSetPortTr. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33265**		
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_8004776c in /formVirtualApp. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33266**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--201221/958
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_80034d60 in /formStaticDHCP. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33267**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--201221/959
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function sub_8003183C in /fromLogin. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33268**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--201221/960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_8004776c in /formVirtualServ. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33269**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--201221/961
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_800462c4 in /formAdvFirewall. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33270**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--201221/962
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function sub_80046EB4 in /formSetPortTr. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33271**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--201221/963
Out-of-bounds Write	01-Dec-21	10	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--201221/964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function FUN_80040af8 in /formWlanSetup. This vulnerability is triggered via a crafted POST request. **CVE ID : CVE-2021-33274**		
elecom					
edwrc-2533gst2_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-EDWR-201221/965
Cross-Site Request	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in	https://www.elecom.co.j	O-ELE-EDWR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**	p/news/security/20211130-01/	201221/966
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-EDWR-201221/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-EDWR-201221/968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-EDWR-201221/969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors.	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-EDWR-201221/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20864		
wrc-1167gst2a_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/971
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/976
wrc-1167gst2h_firmware					
Improper Neutralization of Special	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A	https://www.elecom.co.jp/news/secu	O-ELE-WRC--201221/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**	rity/20211130-01/	
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/981
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2	https://www.elecom.co.jp/news/secu	O-ELE-WRC--201221/982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**	rity/20211130-01/	
wrc-1167gst2_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/986
Improper	01-Dec-21	7.7	OS command injection	https://ww	O-ELE-WRC--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**	w.elecom.co.jp/news/security/20211130-01/	201221/987
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-1750gsv_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/992
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-1750gs_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page.	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20860		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/997
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-1900gst_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1002
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-2533ghbk-i_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	3.5	Cross-site scripting vulnerability in ELECOM LAN router WRC-2533GHBK-I firmware v1.20 and prior allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20857**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1007
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	3.5	Cross-site scripting vulnerability in ELECOM LAN router WRC-2533GHBK-I firmware v1.20 and prior allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20858**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1008
wrc-2533gs2-b_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1012
Improper Neutralization of Special Elements	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior,	https://www.elecom.co.jp/news/security/202111	O-ELE-WRC--201221/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**	30-01/	
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-2533gs2-w_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1017
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2	https://www.elecom.co.jp/news/secu	O-ELE-WRC--201221/1018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**	rity/20211130-01/	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-2533gst2-g_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior)	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1022
Improper Authenticati	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN	https://www.elecom.co.j	O-ELE-WRC--201221/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**	p/news/security/20211130-01/	
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-2533gst2sp_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1028
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior,	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrc-2533gst2_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1033
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**		
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1038
wrc-2533gsta_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1039
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1044
wrc-2533gst_firmware					
Improper Neutralization of Special Elements used in an OS Command	01-Dec-21	7.7	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20859**		
Cross-Site Request Forgery (CSRF)	01-Dec-21	6.8	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page. **CVE ID : CVE-2021-20860**		
Improper Authentication	01-Dec-21	5.8	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors. **CVE ID : CVE-2021-20861**		
Incorrect Authorization	01-Dec-21	3.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unspecified vectors. **CVE ID : CVE-2021-20862**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	7.7	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors. **CVE ID : CVE-2021-20863**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1049
Incorrect Authorization	01-Dec-21	8.3	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRC--201221/1050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20864**		
wrh-733gbk_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Dec-21	5.2	Buffer overflow vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20852**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRH--201221/1051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	5.2	ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute arbitrary OS commands via unspecified vectors. **CVE ID : CVE-2021-20853**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRH--201221/1052
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	5.2	ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute arbitrary OS commands via unspecified vectors. **CVE ID : CVE-2021-20854**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRH--201221/1053
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	3.5	Cross-site scripting vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20855**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRH--201221/1054
Improper Neutralization of Input During Web Page Generation ('Cross-site	01-Dec-21	3.5	Cross-site scripting vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a remote authenticated	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRH--201221/1055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20856**		
wrh-733gwh_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Dec-21	5.2	Buffer overflow vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20852**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRH--201221/1056
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	5.2	ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute arbitrary OS commands via unspecified vectors. **CVE ID : CVE-2021-20853**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRH--201221/1057
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-21	5.2	ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute arbitrary OS commands via unspecified vectors. **CVE ID : CVE-2021-20854**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRH--201221/1058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	3.5	Cross-site scripting vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20855**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRH--201221/1059
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	3.5	Cross-site scripting vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20856**	https://www.elecom.co.jp/news/security/20211130-01/	O-ELE-WRH--201221/1060
fatpipeinc					
ipvpn_firmware					
Unrestricted Upload of File with Dangerous Type	08-Dec-21	9.3	A vulnerability in the web management interface of FatPipe WARP, IPVPN, and MPVPN software prior to versions 10.1.2r60p92 and 10.2.2r44p1 could allow a remote, unauthenticated attacker to upload a file to any location on the filesystem. The FatPipe advisory identifier for this vulnerability is FPSA006. **CVE ID : CVE-2021-27860**	https://www.fatpipeinc.com/support/cve-list.php	O-FAT-IPVP-201221/1061
mpvpn_firmware					
Unrestricted Upload of	08-Dec-21	9.3	A vulnerability in the web management interface of	https://www.fatpipeinc.	O-FAT-MPVP-201221/1062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			FatPipe WARP, IPVPN, and MPVPN software prior to versions 10.1.2r60p92 and 10.2.2r44p1 could allow a remote, unauthenticated attacker to upload a file to any location on the filesystem. The FatPipe advisory identifier for this vulnerability is FPSA006. **CVE ID : CVE-2021-27860**	com/support/cve-list.php	
warp_firmware					
Unrestricted Upload of File with Dangerous Type	08-Dec-21	9.3	A vulnerability in the web management interface of FatPipe WARP, IPVPN, and MPVPN software prior to versions 10.1.2r60p92 and 10.2.2r44p1 could allow a remote, unauthenticated attacker to upload a file to any location on the filesystem. The FatPipe advisory identifier for this vulnerability is FPSA006. **CVE ID : CVE-2021-27860**	https://www.fatpipeinc.com/support/cve-list.php	O-FAT-WARP-201221/1063
Fedoraproject					
fedora					
Heap-based Buffer Overflow	01-Dec-21	6.8	vim is vulnerable to Heap-based Buffer Overflow **CVE ID : CVE-2021-4019**	https://github.com/vim/vim/commit/bd228fd097b41a798f90944b5d1245eddd484142, https://huntr.dev/bounties/d8798584-a6c9-4619-b18f-	O-FED-FEDO-201221/1064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				001b9a6fca92	
Use After Free	06-Dec-21	6.8	vim is vulnerable to Use After Free **CVE ID : CVE-2021-4069**	https://huntr.dev/bounties/0efd6d23-2259-4081-9ff1-3ade26907d74, https://github.com/vim/vim/commit/e031fe90cf2e375ce861ff5e5e281e4ad229ebb9	O-FED-FEDO-201221/1065
Fortinet					
fortios					
Out-of-bounds Write	08-Dec-21	6.8	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images. **CVE ID : CVE-2021-36173**	https://fortiguard.com/advisory/FG-IR-21-115	O-FOR-FORT-201221/1066
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-21	5	A relative path traversal [CWE-23] vulnerabiltiy in FortiOS versions 7.0.0 and 7.0.1 and FortiProxy verison 7.0.0 may allow an unauthenticated, unauthorized attacker to inject path traversal character sequences to disclose sensitive information	https://fortiguard.com/advisory/FG-IR-21-181	O-FOR-FORT-201221/1067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the server via the GET request of the login page. **CVE ID : CVE-2021-41024**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	4.6	A buffer overflow [CWE-121] in the TFTP client library of FortiOS before 6.4.7 and FortiOS 7.0.0 through 7.0.2, may allow an authenticated local attacker to achieve arbitrary code execution via specially crafted command line arguments. **CVE ID : CVE-2021-42757**	https://fortiguard.com/advisory/FG-IR-21-173	O-FOR-FORT-201221/1068
Insufficient Verification of Data Authenticity	08-Dec-21	5.1	An insufficient verification of data authenticity vulnerability (CWE-345) in the user interface of FortiProxy verison 2.0.3 and below, 1.2.11 and below and FortiGate verison 7.0.0, 6.4.6 and below, 6.2.9 and below of SSL VPN portal may allow a remote, unauthenticated attacker to conduct a cross-site request forgery (CSRF) attack . Only SSL VPN in web mode or full mode are impacted by this vulnerability. **CVE ID : CVE-2021-26103**	https://fortiguard.com/advisory/FG-IR-20-158	O-FOR-FORT-201221/1069
Use of Hard-coded Credentials	08-Dec-21	5	A use of hard-coded cryptographic key vulnerability in the SSLVPN of FortiOS before 7.0.1 may allow an attacker to retrieve the key by reverse engineering. **CVE ID : CVE-2021-26108**	https://fortiguard.com/advisory/FG-IR-21-051	O-FOR-FORT-201221/1070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Dec-21	7.5	An integer overflow or wraparound vulnerability in the memory allocator of SSLVPN in FortiOS before 7.0.1 may allow an unauthenticated attacker to corrupt control data on the heap via specifically crafted requests to SSLVPN, resulting in potentially arbitrary code execution. **CVE ID : CVE-2021-26109**	https://fortiguard.com/advisory/FG-IR-21-049	O-FOR-FORT-201221/1071
Improper Privilege Management	08-Dec-21	4.6	An improper access control vulnerability [CWE-284] in FortiOS autod daemon 7.0.0, 6.4.6 and below, 6.2.9 and below, 6.0.12 and below and FortiProxy 2.0.1 and below, 1.2.9 and below may allow an authenticated low-privileged attacker to escalate their privileges to super_admin via a specific crafted configuration of fabric automation CLI script and auto-script features. **CVE ID : CVE-2021-26110**	https://fortiguard.com/advisory/FG-IR-20-131	O-FOR-FORT-201221/1072
meru_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	7.2	A violation of secure design principles in Fortinet Meru AP version 8.6.1 and below, version 8.5.5 and below allows attacker to execute unauthorized code or commands via crafted cli commands. **CVE ID : CVE-2021-42759**	https://fortiguard.com/advisory/FG-IR-21-004	O-FOR-MERU-201221/1073
gl-inet					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gl-ar150_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-21	4.3	GL.iNet GL-AR150 2.x before 3.x devices, configured as repeaters, allow cgi-bin/router_cgi?action=scanwifi XSS when an attacker creates an SSID with an XSS payload as the name. **CVE ID : CVE-2021-44148**	https://beaugraham.com/CVE-2021-44148-xss.html	O-GL--GL-A-201221/1074
Google					
android					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	A Universal XSS vulnerability was present in Firefox for Android resulting from improper sanitization when processing a URL scanned from a QR code. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 94. **CVE ID : CVE-2021-43530**	https://www.mozilla.org/security/advisories/mfsa2021-48/	O-GOO-ANDR-201221/1075
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-21	4.3	When receiving a URL through a SEND intent, Firefox would have searched for the text, but subsequent usages of the address bar might have caused the URL to load unintentionally, which could lead to XSS and spoofing attacks. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 95. **CVE ID : CVE-2021-43544**	https://www.mozilla.org/security/advisories/mfsa2021-52/	O-GOO-ANDR-201221/1076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Dec-21	4.6	An improper validation vulnerability in FilterProvider prior to SMR Dec-2021 Release 1 allows local arbitrary code execution. **CVE ID : CVE-2021-25510**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=12	O-GOO-ANDR-201221/1077
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-21	4.6	An improper validation vulnerability in FilterProvider prior to SMR Dec-2021 Release 1 allows attackers to write arbitrary files via a path traversal vulnerability. **CVE ID : CVE-2021-25511**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=12	O-GOO-ANDR-201221/1078
Improper Input Validation	08-Dec-21	4.6	An improper validation vulnerability in telephony prior to SMR Dec-2021 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2021-25512**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=12	O-GOO-ANDR-201221/1079
Improper Privilege Management	08-Dec-21	2.1	An improper privilege management vulnerability in Apps Edge application prior to SMR Dec-2021 Release 1 allows unauthorized access to some device data on the lockscreen. **CVE ID : CVE-2021-25513**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=12	O-GOO-ANDR-201221/1080
N/A	08-Dec-21	4.3	An improper intent redirection handling in Tags prior to SMR Dec-2021 Release 1 allows attackers to access sensitive information. **CVE ID : CVE-2021-25514**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=12	O-GOO-ANDR-201221/1081
Improper	08-Dec-21	2.1	An improper usage of implicit	https://secu	O-GOO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			intent in SemRewardManager prior to SMR Dec-2021 Release 1 allows attackers to access BSSID. **CVE ID : CVE-2021-25515**	rity.samsung mobile.com/ securityUpda te.smsb?year =2021&mont h=12	ANDR-201221/1082
Improper Handling of Exceptional Conditions	08-Dec-21	5	An improper check or handling of exceptional conditions in Exynos baseband prior to SMR Dec-2021 Release 1 allows attackers to track locations. **CVE ID : CVE-2021-25516**	https://secu rity.samsung mobile.com/ securityUpda te.smsb?year =2021&mont h=12	O-GOO-ANDR-201221/1083
Improper Input Validation	08-Dec-21	4.6	An improper input validation vulnerability in LDFW prior to SMR Dec-2021 Release 1 allows attackers to perform arbitrary code execution. **CVE ID : CVE-2021-25517**	https://secu rity.samsung mobile.com/ securityUpda te.smsb?year =2021&mont h=12	O-GOO-ANDR-201221/1084
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Dec-21	4.6	An improper boundary check in secure_log of LDFW and BL31 prior to SMR Dec-2021 Release 1 allows arbitrary memory write and code execution. **CVE ID : CVE-2021-25518**	https://secu rity.samsung mobile.com/ securityUpda te.smsb?year =2021&mont h=12	O-GOO-ANDR-201221/1085
Incorrect Permission Assignment for Critical Resource	08-Dec-21	2.1	An improper access control vulnerability in CPLC prior to SMR Dec-2021 Release 1 allows local attackers to access CPLC information without permission. **CVE ID : CVE-2021-25519**	https://secu rity.samsung mobile.com/ securityUpda te.smsb?year =2021&mont h=12	O-GOO-ANDR-201221/1086
gryphonconnect					
gryphon_tower_firmware					
Improper	09-Dec-21	4.3	A reflected cross-site	N/A	O-GRY-GRYP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			scripting vulnerability exists in the url parameter of the /cgi-bin/luci/site_access/ page on the Gryphon Tower router's web interface. An attacker could exploit this issue by tricking a user into following a specially crafted link, granting the attacker javascript execution in the context of the victim's browser. **CVE ID : CVE-2021-20137**		201221/1087
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	8.3	An unauthenticated command injection vulnerability exists in multiple parameters in the Gryphon Tower router's web interface at /cgi-bin/luci/rc. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the web interface. **CVE ID : CVE-2021-20138**	https://www.tenable.com/security/research/tra-2021-51	O-GRY-GRYP-201221/1088
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	8.3	An unauthenticated command injection vulnerability exists in the parameters of operation 3 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999.	https://www.tenable.com/security/research/tra-2021-51	O-GRY-GRYP-201221/1089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20139		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	8.3	An unauthenticated command injection vulnerability exists in the parameters of operation 10 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999. **CVE ID : CVE-2021-20140**	https://www.tenable.com/security/research/tra-2021-51	O-GRY-GRYP-201221/1090
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	8.3	An unauthenticated command injection vulnerability exists in the parameters of operation 32 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999. **CVE ID : CVE-2021-20141**	https://www.tenable.com/security/research/tra-2021-51	O-GRY-GRYP-201221/1091
Improper Neutralization of Special Elements used in an OS Command ('OS Command	09-Dec-21	8.3	An unauthenticated command injection vulnerability exists in the parameters of operation 41 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network	https://www.tenable.com/security/research/tra-2021-51	O-GRY-GRYP-201221/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999. **CVE ID : CVE-2021-20142**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	8.3	An unauthenticated command injection vulnerability exists in the parameters of operation 48 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999. **CVE ID : CVE-2021-20143**	https://www.tenable.com/security/research/tra-2021-51	O-GRY-GRYP-201221/1093
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Dec-21	8.3	An unauthenticated command injection vulnerability exists in the parameters of operation 49 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999. **CVE ID : CVE-2021-20144**	https://www.tenable.com/security/research/tra-2021-51	O-GRY-GRYP-201221/1094
Improper Authenticati	09-Dec-21	5	Gryphon Tower routers contain an unprotected	https://www.tenable.co	O-GRY-GRYP-201221/1095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			openvpn configuration file which can grant attackers access to the Gryphon homebound VPN network which exposes the LAN interfaces of other users' devices connected to the same service. An attacker could leverage this to make configuration changes to, or otherwise attack victims' devices as though they were on an adjacent network. **CVE ID : CVE-2021-20145**	m/security/research/tra-2021-51	
Insufficiently Protected Credentials	09-Dec-21	10	An unprotected ssh private key exists on the Gryphon devices which could be used to achieve root access to a server affiliated with Gryphon's development and infrastructure. At the time of discovery, the ssh key could be used to login to the development server hosted in Amazon Web Services. **CVE ID : CVE-2021-20146**	https://www.tenable.com/security/research/tra-2021-51	O-GRY-GRYP-201221/1096
hitachienergy					
fox615_firmware					
Weak Password Requirements	02-Dec-21	5.5	Weak Password Requirements vulnerability in Hitachi Energy FOX61x, XCM20 allows an attacker to gain unauthorized access to the Data Communication Network (DCN) routing configuration. This issue affects: Hitachi Energy FOX61x versions prior to R15A. Hitachi Energy XCM20	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000062&LanguageCode=en&DocumentPartId=&Action=Launch,	O-HIT-FOX6-201221/1097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to R15A. **CVE ID : CVE-2021-40333**	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000069&LanguageCode=en&DocumentPartId=&Action=Launch	
N/A	02-Dec-21	5	Missing Handler vulnerability in the proprietary management protocol (port TCP 5558) of Hitachi Energy FOX61x, XCM20 allows an attacker that exploits the vulnerability by activating SSH on port TCP 5558 to cause disruption to the NMS and NE communication. This issue affects: Hitachi Energy FOX61x versions prior to R15A. Hitachi Energy XCM20 versions prior to R15A. **CVE ID : CVE-2021-40334**	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000062&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000069&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-FOX6-201221/1098
xcm20_firmware					
Weak Password Requirements	02-Dec-21	5.5	Weak Password Requirements vulnerability in Hitachi Energy FOX61x, XCM20 allows an attacker to gain unauthorized access to the Data Communication	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000062	O-HIT-XCM2-201221/1099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Network (DCN) routing configuration. This issue affects: Hitachi Energy FOX61x versions prior to R15A. Hitachi Energy XCM20 versions prior to R15A. **CVE ID : CVE-2021-40333**	&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000069&LanguageCode=en&DocumentPartId=&Action=Launch	
N/A	02-Dec-21	5	Missing Handler vulnerability in the proprietary management protocol (port TCP 5558) of Hitachi Energy FOX61x, XCM20 allows an attacker that exploits the vulnerability by activating SSH on port TCP 5558 to cause disruption to the NMS and NE communication. This issue affects: Hitachi Energy FOX61x versions prior to R15A. Hitachi Energy XCM20 versions prior to R15A. **CVE ID : CVE-2021-40334**	https://search.abb.com/library/Download.aspx?DocumentID=8DBD000062&LanguageCode=en&DocumentPartId=&Action=Launch, https://search.abb.com/library/Download.aspx?DocumentID=8DBD000069&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-XCM2-201221/1100
HP					
hp-ux					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-Dec-21	2.1	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to gain privileges due to allowing modification of columns of existing tasks. IBM X-Force ID: 210321. **CVE ID : CVE-2021-38926**	https://exchange.xforce.ibmcloud.com/vulnerabilities/210321, https://www.ibm.com/support/pages/node/6523808	O-HP-HP-U-201221/1101
Exposure of Resource to Wrong Sphere	09-Dec-21	4	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1, and 11.5 is vulnerable to an information disclosure as a result of a connected user having indirect read access to a table where they are not authorized to select from. IBM X-Force ID: 210418. **CVE ID : CVE-2021-38931**	https://www.ibm.com/support/pages/node/6523810, https://exchange.xforce.ibmcloud.com/vulnerabilities/210418	O-HP-HP-U-201221/1102
Uncontrolled Resource Consumption	09-Dec-21	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available CPU resources. IBM X-Force ID: 211405. **CVE ID : CVE-2021-38951**	https://www.ibm.com/support/pages/node/6524674, https://exchange.xforce.ibmcloud.com/vulnerabilities/211405	O-HP-HP-U-201221/1103
Use of a Broken or Risky Cryptographic Algorithm	09-Dec-21	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 uses weaker than expected cryptographic algorithms that could allow an attacker to	https://exchange.xforce.ibmcloud.com/vulnerabilities/213217, https://www.ibm.com/s	O-HP-HP-U-201221/1104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			decrypt highly sensitive information. **CVE ID : CVE-2021-39002**	upport/pages/node/6523802	
Exposure of Resource to Wrong Sphere	09-Dec-21	5	IBM Db2 9.7, 10.1, 10.5, 11.1, and 11.5 may be vulnerable to an Information Disclosure when using the LOAD utility as under certain circumstances the LOAD utility does not enforce directory restrictions. IBM X-Force ID: 199521. **CVE ID : CVE-2021-20373**	https://www.ibm.com/support/pages/node/6523804, https://exchange.xforce.ibmcloud.com/vulnerabilities/195521	O-HP-HP-U-201221/1105
Incorrect Authorization	09-Dec-21	5.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a user with DBADM authority to access other databases and read or modify files. IBM X-Force ID: 199914. **CVE ID : CVE-2021-29678**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199914, https://www.ibm.com/support/pages/node/6523806	O-HP-HP-U-201221/1106
Huawei					
emui					
Improper Input Validation	07-Dec-21	6.4	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Out-of-bounds read. **CVE ID : CVE-2021-37020**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-EMUI-201221/1107
Improper Input Validation	07-Dec-21	6.4	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful	https://device.harmonyos.com/en/docs/security/u	O-HUA-EMUI-201221/1108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may lead to Out-of-bounds read. **CVE ID : CVE-2021-37021**	pdate/security-bulletins-202109-0000001196270727	
N/A	08-Dec-21	7.8	There is an Invalid address access vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the device to restart. **CVE ID : CVE-2021-37037**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-EMUI-201221/1109
Incorrect Authorization	07-Dec-21	5	There is an Improper access control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2021-37038**	https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-EMUI-201221/1110
Improper Input Validation	08-Dec-21	3.3	There is an Input verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause Bluetooth DoS. **CVE ID : CVE-2021-37039**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin	O-HUA-EMUI-201221/1111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/2021/9/	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Dec-21	6.8	There is a Parameter injection vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause privilege escalation of files after CIFS share mounting. **CVE ID : CVE-2021-37040**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-EMUI-201221/1112
Improper Input Validation	07-Dec-21	6.4	There is an Improper verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause out-of-bounds read. **CVE ID : CVE-2021-37041**	https://consumer.huawei.com/en/support/bulletin/2021/9/, https://consumer.huawei.com/om/support/bulletin/2021/10/	O-HUA-EMUI-201221/1113
Improper Input Validation	07-Dec-21	6.4	There is an Improper verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause out-of-bounds read. **CVE ID : CVE-2021-37042**	https://consumer.huawei.com/en/support/bulletin/2021/9/, https://consumer.huawei.com/om/support/bulletin/2021/10/	O-HUA-EMUI-201221/1114
Improper Authentication	07-Dec-21	5	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this	https://device.harmonyos.com/en/docs/security/update/securi	O-HUA-EMUI-201221/1115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may lead to malicious application processes occupy system resources. **CVE ID : CVE-2021-37043**	ty-bulletins-202109-0000001196270727	
Improper Preservation of Permissions	08-Dec-21	5	There is a Permission control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability. **CVE ID : CVE-2021-37044**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-EMUI-201221/1116
N/A	08-Dec-21	10	There is an UAF vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the device to restart unexpectedly and the kernel-mode code to be executed. **CVE ID : CVE-2021-37045**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-EMUI-201221/1117
Missing Release of Memory after Effective Lifetime	07-Dec-21	7.8	There is a Memory leak vulnerability with the codec detection module in Huawei Smartphone.Successful exploitation of this vulnerability may cause the device to restart due to	https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-EMUI-201221/1118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory exhaustion. **CVE ID : CVE-2021-37046**		
Improper Input Validation	07-Dec-21	5	There is an Input verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause some services to restart. **CVE ID : CVE-2021-37047**	https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-EMUI-201221/1119
Out-of-bounds Write	08-Dec-21	7.5	There is a Heap-based buffer overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may rewrite the memory of adjacent objects. **CVE ID : CVE-2021-37049**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-000000119627072 7, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-EMUI-201221/1120
Missing Encryption of Sensitive Data	08-Dec-21	5	There is a Missing sensitive data encryption vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2021-37050**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-000000119627072 7, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-EMUI-201221/1121
Out-of-bounds Read	08-Dec-21	6.4	There is an Out-of-bounds read vulnerability in Huawei	https://device.harmonyos.	O-HUA-EMUI-201221/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Smartphone.Successful exploitation of this vulnerability may cause out-of-bounds memory access. **CVE ID : CVE-2021-37051**	com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/, https://consumer.huawei.com/en/support/bulletin/2021/10/	
Improper Handling of Exceptional Conditions	08-Dec-21	5	There is an Exception log vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause address information leakage. **CVE ID : CVE-2021-37052**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-EMUI-201221/1123
N/A	08-Dec-21	5	There is a Service logic vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause WLAN DoS. **CVE ID : CVE-2021-37053**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727,	O-HUA-EMUI-201221/1124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://consumer.huawei.com/en/support/bulletin/2021/9/, https://consumer.huawei.com/en/support/bulletin/2021/10/	
Improper Authentication	08-Dec-21	5	There is an Identity spoofing and authentication bypass vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2021-37054**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-000000119627072 7, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-EMUI-201221/1125
N/A	07-Dec-21	5	There is a Logic bypass vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may allow attempts to obtain certain device information. **CVE ID : CVE-2021-37055**	https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-EMUI-201221/1126
Improper Preservation of Permissions	07-Dec-21	5	There is an Improper permission control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may allow attempts to obtain certain	https://consumer.huawei.com/en/support/bulletin/2021/9/, https://consumer.huawei.com/om/su	O-HUA-EMUI-201221/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device information. **CVE ID : CVE-2021-37056**	pport/bulletin/2021/10/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Dec-21	5.8	There is a Race Condition vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to availability affected. **CVE ID : CVE-2021-37069**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/11/	O-HUA-EMUI-201221/1128
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Dec-21	9.3	There is a Race Condition vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to the user root privilege escalation. **CVE ID : CVE-2021-37074**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/11/	O-HUA-EMUI-201221/1129
Insufficiently Protected Credentials	08-Dec-21	5	There is a Credentials Management Errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to confidentiality affected. **CVE ID : CVE-2021-37075**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://cons	O-HUA-EMUI-201221/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				umer.huawei.com/en/support/bulletin/2021/10/	
Incomplete Cleanup	08-Dec-21	5	There is a Incomplete Cleanup vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to availability affected. **CVE ID : CVE-2021-37092**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/10/	O-HUA-EMUI-201221/1131
N/A	08-Dec-21	5	There is a Improper Access Control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to attackers steal short messages. **CVE ID : CVE-2021-37093**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/10/	O-HUA-EMUI-201221/1132
Improper Control of Generation of Code ('Code Injection')	08-Dec-21	7.8	There is a Code Injection vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to system restart. **CVE ID : CVE-2021-37097**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196	O-HUA-EMUI-201221/1133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				270727, https://consumer.huawei.com/en/support/bulletin/2021/10/	
harmonyos					
Out-of-bounds Write	07-Dec-21	9.4	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Out-of-bounds read. **CVE ID : CVE-2021-37011**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1134
Integer Overflow or Wraparound	07-Dec-21	5	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to device cannot be used properly. **CVE ID : CVE-2021-37014**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1135
Improper Input Validation	07-Dec-21	6.4	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Out-of-bounds read. **CVE ID : CVE-2021-37020**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1136
Improper Input Validation	07-Dec-21	6.4	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this	https://device.harmonyos.com/en/docs/security/update/securi	O-HUA-HARM-201221/1137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may lead to Out-of-bounds read. **CVE ID : CVE-2021-37021**	ty-bulletins-202109-0000001196270727	
N/A	08-Dec-21	7.8	There is an Invalid address access vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the device to restart. **CVE ID : CVE-2021-37037**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-HARM-201221/1138
Improper Input Validation	08-Dec-21	3.3	There is an Input verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause Bluetooth DoS. **CVE ID : CVE-2021-37039**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-HARM-201221/1139
Improper Neutralization of Special Elements in Output Used by a Downstream Component	08-Dec-21	6.8	There is a Parameter injection vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause privilege escalation of files after CIFS share mounting.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196	O-HUA-HARM-201221/1140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			**CVE ID : CVE-2021-37040**	270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	
Improper Authentication	07-Dec-21	5	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to malicious application processes occupy system resources. **CVE ID : CVE-2021-37043**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1141
Improper Preservation of Permissions	08-Dec-21	5	There is a Permission control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability. **CVE ID : CVE-2021-37044**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-HARM-201221/1142
N/A	08-Dec-21	10	There is an UAF vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the device to restart unexpectedly and the kernel-mode code to be executed. **CVE ID : CVE-2021-37045**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://cons	O-HUA-HARM-201221/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				umer.huawei.com/en/support/bulletin/2021/9/	
Improper Input Validation	07-Dec-21	5	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to fake visitors to control PC,play a video,etc. **CVE ID : CVE-2021-37048**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1144
Out-of-bounds Write	08-Dec-21	7.5	There is a Heap-based buffer overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may rewrite the memory of adjacent objects. **CVE ID : CVE-2021-37049**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-HARM-201221/1145
Missing Encryption of Sensitive Data	08-Dec-21	5	There is a Missing sensitive data encryption vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2021-37050**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin	O-HUA-HARM-201221/1146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/2021/9/	
Out-of-bounds Read	08-Dec-21	6.4	There is an Out-of-bounds read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause out-of-bounds memory access. **CVE ID : CVE-2021-37051**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/, https://consumer.huawei.com/en/support/bulletin/2021/10/	O-HUA-HARM-201221/1147
Improper Handling of Exceptional Conditions	08-Dec-21	5	There is an Exception log vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause address information leakage. **CVE ID : CVE-2021-37052**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-HARM-201221/1148
N/A	08-Dec-21	5	There is a Service logic vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause WLAN DoS.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-	O-HUA-HARM-201221/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-37053	202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/, https://consumer.huawei.com/en/support/bulletin/2021/10/	
Improper Authentication	08-Dec-21	5	There is an Identity spoofing and authentication bypass vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2021-37054**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-HARM-201221/1150
Improper Validation of Array Index	07-Dec-21	7.8	There is a Improper Validation of Array Index vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to restart the phone. **CVE ID : CVE-2021-37057**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1151
Incorrect Permission Assignment for Critical	07-Dec-21	5	There is a Permissions,Privileges,and Access Controls vulnerability in Huawei	https://device.harmonyos.com/en/docs/security/u	O-HUA-HARM-201221/1152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource			Smartphone.Successful exploitation of this vulnerability may lead to the user's nickname is maliciously tampered with. **CVE ID : CVE-2021-37058**	pdate/security-bulletins-202109-0000001196270727	
N/A	07-Dec-21	7.5	There is a Weaknesses Introduced During Design **CVE ID : CVE-2021-37059**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1153
Improper Input Validation	07-Dec-21	5	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to SAMGR Heap Address Leakage. **CVE ID : CVE-2021-37060**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1154
Uncontrolled Resource Consumption	07-Dec-21	5	There is a Uncontrolled Resource Consumption vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Screen projection application denial of service. **CVE ID : CVE-2021-37061**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1155
Improper Validation of Array Index	07-Dec-21	6.4	There is a Improper Validation of Array Index vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to	https://device.harmonyos.com/en/docs/security/update/security-bulletins-	O-HUA-HARM-201221/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory overflow and information leakage. **CVE ID : CVE-2021-37062**	202109-0000001196270727	
N/A	07-Dec-21	7.5	There is a Cryptographic Issues vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to read and delete images of Harmony devices. **CVE ID : CVE-2021-37063**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1157
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Dec-21	6.4	There is a Improper Limitation of a Pathname to a Restricted Directory vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to arbitrary file created. **CVE ID : CVE-2021-37064**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1158
Integer Overflow or Wraparound	07-Dec-21	6.4	There is a Integer Overflow or Wraparound vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Confidentiality or Availability impacted. **CVE ID : CVE-2021-37065**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1159
Out-of-bounds Read	07-Dec-21	5	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to process crash. **CVE ID : CVE-2021-37066**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196	O-HUA-HARM-201221/1160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				270727	
Exposure of Sensitive Information to an Unauthorized Actor	07-Dec-21	5	There is a Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Confidentiality impacted. **CVE ID : CVE-2021-37067**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1161
Uncontrolled Resource Consumption	07-Dec-21	5	There is a Resource Management Errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to denial of Service Attacks. **CVE ID : CVE-2021-37068**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1162
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Dec-21	5.8	There is a Race Condition vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to availability affected. **CVE ID : CVE-2021-37069**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/11/	O-HUA-HARM-201221/1163
Out-of-bounds Read	07-Dec-21	5	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to process crash.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-	O-HUA-HARM-201221/1164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-37070	202109-0000001196270727	
N/A	07-Dec-21	5	There is a Business Logic Errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to persistent dos. **CVE ID : CVE-2021-37071**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1165
Double Free	07-Dec-21	5	There is a Incorrect Calculation of Buffer Size vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to memory crash. **CVE ID : CVE-2021-37072**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1166
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	07-Dec-21	4.3	There is a Race Condition vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to the detection result is tampered with. **CVE ID : CVE-2021-37073**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1167
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Dec-21	9.3	There is a Race Condition vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to the user root privilege escalation. **CVE ID : CVE-2021-37074**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://cons	O-HUA-HARM-201221/1168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				umer.huawei.com/en/support/bulletin/2021/11/	
Insufficiently Protected Credentials	08-Dec-21	5	There is a Credentials Management Errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to confidentiality affected. **CVE ID : CVE-2021-37075**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/10/	O-HUA-HARM-201221/1169
Out-of-bounds Read	07-Dec-21	5	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to availability affected. **CVE ID : CVE-2021-37076**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1170
NULL Pointer Dereference	07-Dec-21	7.8	There is a NULL Pointer Dereference vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to kernel crash. **CVE ID : CVE-2021-37077**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1171
N/A	07-Dec-21	5	There is a Uncaught Exception vulnerability in Huawei Smartphone.Successful	https://device.harmonyos.com/en/docs/security/u	O-HUA-HARM-201221/1172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may lead to remote Denial of Service. **CVE ID : CVE-2021-37078**	pdate/security-bulletins-202109-0000001196270727	
Improper Input Validation	07-Dec-21	6.4	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to delete arbitrary file by system_app permission. **CVE ID : CVE-2021-37079**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1173
Incomplete Cleanup	07-Dec-21	5	There is a Incomplete Cleanup vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to availability affected. **CVE ID : CVE-2021-37080**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1174
Improper Input Validation	07-Dec-21	5	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to nearby crash. **CVE ID : CVE-2021-37081**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1175
Concurrent Execution using Shared Resource with Improper Synchronizat	07-Dec-21	4.3	There is a Race Condition vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to motionhub crash. **CVE ID : CVE-2021-37082**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-	O-HUA-HARM-201221/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion ('Race Condition')				0000001196270727	
NULL Pointer Dereference	07-Dec-21	5	There is a NULL Pointer Dereference vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Denial of Service Attacks. **CVE ID : CVE-2021-37083**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1177
Improper Input Validation	07-Dec-21	7.5	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to malicious invoking other functions of the Smart Assistant through text messages. **CVE ID : CVE-2021-37084**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1178
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	07-Dec-21	7.1	There is a Encoding timing vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to denial of service. **CVE ID : CVE-2021-37085**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1179
Improper Preservation of Permissions	07-Dec-21	5	There is a Improper Preservation of Permissions vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to attackers which can isolate and read synchronization	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196	O-HUA-HARM-201221/1180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			files of other applications across the UID sandbox. **CVE ID : CVE-2021-37086**	270727	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Dec-21	6.4	There is a Path Traversal vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to attackers can create arbitrary file. **CVE ID : CVE-2021-37087**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1181
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Dec-21	6.4	There is a Path Traversal vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to attackers can write any content to any file. **CVE ID : CVE-2021-37088**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1182
Incomplete Cleanup	07-Dec-21	7.8	There is a Incomplete Cleanup vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to kernel restart. **CVE ID : CVE-2021-37089**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1183
Out-of-bounds Read	07-Dec-21	5	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to process crash. **CVE ID : CVE-2021-37090**	N/A	O-HUA-HARM-201221/1184
Improper Privilege	07-Dec-21	5	There is a Permissions,Privileges,and	https://device.harmonyos.	O-HUA-HARM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Access Controls vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to confidentiality affected. **CVE ID : CVE-2021-37091**	com/en/docs/security/update/security-bulletins-202109-0000001196270727	201221/1185
Incomplete Cleanup	08-Dec-21	5	There is a Incomplete Cleanup vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to availability affected. **CVE ID : CVE-2021-37092**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/10/	O-HUA-HARM-201221/1186
N/A	08-Dec-21	5	There is a Improper Access Control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to attackers steal short messages. **CVE ID : CVE-2021-37093**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/10/	O-HUA-HARM-201221/1187
Improper Input Validation	07-Dec-21	5	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this	https://device.harmonyos.com/en/docs/security/update/securi	O-HUA-HARM-201221/1188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may lead to system denial of service. **CVE ID : CVE-2021-37094**	ty-bulletins-202109-0000001196270727	
Integer Overflow or Wraparound	07-Dec-21	7.5	There is a Integer Overflow or Wraparound vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to remote denial of service and potential remote code execution. **CVE ID : CVE-2021-37095**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1189
Improper Input Validation	07-Dec-21	5	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to user privacy disclosed. **CVE ID : CVE-2021-37096**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1190
Improper Control of Generation of Code ('Code Injection')	08-Dec-21	7.8	There is a Code Injection vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to system restart. **CVE ID : CVE-2021-37097**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/10/	O-HUA-HARM-201221/1191
Improper Limitation of	07-Dec-21	6.4	There is a Path Traversal vulnerability in Huawei	https://device.harmonyos.	O-HUA-HARM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			Smartphone.Successful exploitation of this vulnerability may lead to delete any file. **CVE ID : CVE-2021-37099**	com/en/docs/security/update/security-bulletins-202109-0000001196270727	201221/1192
Improper Authentication	07-Dec-21	5	There is a Improper Authentication vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to account authentication bypassed. **CVE ID : CVE-2021-37100**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-HARM-201221/1193
magic_ui					
Improper Input Validation	07-Dec-21	6.4	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Out-of-bounds read. **CVE ID : CVE-2021-37020**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-MAGI-201221/1194
Improper Input Validation	07-Dec-21	6.4	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Out-of-bounds read. **CVE ID : CVE-2021-37021**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-MAGI-201221/1195
N/A	08-Dec-21	7.8	There is an Invalid address access vulnerability in Huawei Smartphone.Successful	https://device.harmonyos.com/en/docs/security/u	O-HUA-MAGI-201221/1196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may cause the device to restart. **CVE ID : CVE-2021-37037**	pdate/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	
Incorrect Authorization	07-Dec-21	5	There is an Improper access control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2021-37038**	https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-MAGI-201221/1197
Improper Input Validation	08-Dec-21	3.3	There is an Input verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause Bluetooth DoS. **CVE ID : CVE-2021-37039**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-MAGI-201221/1198
Improper Neutralization of Special Elements in Output Used by a Downstream Component	08-Dec-21	6.8	There is a Parameter injection vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause privilege escalation of files	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196	O-HUA-MAGI-201221/1199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			after CIFS share mounting. **CVE ID : CVE-2021-37040**	270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	
Improper Input Validation	07-Dec-21	6.4	There is an Improper verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause out-of-bounds read. **CVE ID : CVE-2021-37041**	https://consumer.huawei.com/en/support/bulletin/2021/9/, https://consumer.huawei.com/om/support/bulletin/2021/10/	O-HUA-MAGI-201221/1200
Improper Input Validation	07-Dec-21	6.4	There is an Improper verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause out-of-bounds read. **CVE ID : CVE-2021-37042**	https://consumer.huawei.com/en/support/bulletin/2021/9/, https://consumer.huawei.com/om/support/bulletin/2021/10/	O-HUA-MAGI-201221/1201
Improper Authentication	07-Dec-21	5	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to malicious application processes occupy system resources. **CVE ID : CVE-2021-37043**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727	O-HUA-MAGI-201221/1202
Improper Preservation of	08-Dec-21	5	There is a Permission control vulnerability in Huawei Smartphone.Successful	https://device.harmonyos.com/en/doc	O-HUA-MAGI-201221/1203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			exploitation of this vulnerability may affect service availability. **CVE ID : CVE-2021-37044**	s/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	
N/A	08-Dec-21	10	There is an UAF vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the device to restart unexpectedly and the kernel-mode code to be executed. **CVE ID : CVE-2021-37045**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-MAGI-201221/1204
Missing Release of Memory after Effective Lifetime	07-Dec-21	7.8	There is a Memory leak vulnerability with the codec detection module in Huawei Smartphone.Successful exploitation of this vulnerability may cause the device to restart due to memory exhaustion. **CVE ID : CVE-2021-37046**	https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-MAGI-201221/1205
Improper Input Validation	07-Dec-21	5	There is an Input verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause some	https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-MAGI-201221/1206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			services to restart. **CVE ID : CVE-2021-37047**		
Out-of-bounds Write	08-Dec-21	7.5	There is a Heap-based buffer overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may rewrite the memory of adjacent objects. **CVE ID : CVE-2021-37049**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-000000119627072 7, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-MAGI-201221/1207
Missing Encryption of Sensitive Data	08-Dec-21	5	There is a Missing sensitive data encryption vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2021-37050**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-000000119627072 7, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-MAGI-201221/1208
Out-of-bounds Read	08-Dec-21	6.4	There is an Out-of-bounds read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause out-of-bounds memory access. **CVE ID : CVE-2021-37051**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-000000119627072 7, https://cons	O-HUA-MAGI-201221/1209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				umer.huawei.com/en/support/bulletin/2021/9/, https://consumer.huawei.com/en/support/bulletin/2021/10/	
Improper Handling of Exceptional Conditions	08-Dec-21	5	There is an Exception log vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause address information leakage. **CVE ID : CVE-2021-37052**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-MAGI-201221/1210
N/A	08-Dec-21	5	There is a Service logic vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause WLAN DoS. **CVE ID : CVE-2021-37053**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/, https://consumer.huawei.com/en/sup	O-HUA-MAGI-201221/1211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				port/bulletin/2021/10/	
Improper Authentication	08-Dec-21	5	There is an Identity spoofing and authentication bypass vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2021-37054**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-MAGI-201221/1212
N/A	07-Dec-21	5	There is a Logic bypass vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may allow attempts to obtain certain device information. **CVE ID : CVE-2021-37055**	https://consumer.huawei.com/en/support/bulletin/2021/9/	O-HUA-MAGI-201221/1213
Improper Preservation of Permissions	07-Dec-21	5	There is an Improper permission control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may allow attempts to obtain certain device information. **CVE ID : CVE-2021-37056**	https://consumer.huawei.com/en/support/bulletin/2021/9/, https://consumer.huawei.com/om/support/bulletin/2021/10/	O-HUA-MAGI-201221/1214
Concurrent Execution using Shared Resource with	08-Dec-21	5.8	There is a Race Condition vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to	https://device.harmonyos.com/en/docs/security/update/securi	O-HUA-MAGI-201221/1215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			availability affected. **CVE ID : CVE-2021-37069**	ty-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/11/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Dec-21	9.3	There is a Race Condition vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to the user root privilege escalation. **CVE ID : CVE-2021-37074**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/11/	O-HUA-MAGI-201221/1216
Insufficiently Protected Credentials	08-Dec-21	5	There is a Credentials Management Errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to confidentiality affected. **CVE ID : CVE-2021-37075**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/10/	O-HUA-MAGI-201221/1217
Incomplete Cleanup	08-Dec-21	5	There is a Incomplete Cleanup vulnerability in Huawei	https://device.harmonyos.com/en/doc	O-HUA-MAGI-201221/1218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Smartphone.Successful exploitation of this vulnerability may lead to availability affected. **CVE ID : CVE-2021-37092**	s/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/10/	
N/A	08-Dec-21	5	There is a Improper Access Control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to attackers steal short messages. **CVE ID : CVE-2021-37093**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/10/	O-HUA-MAGI-201221/1219
Improper Control of Generation of Code ('Code Injection')	08-Dec-21	7.8	There is a Code Injection vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to system restart. **CVE ID : CVE-2021-37097**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202109-0000001196270727, https://consumer.huawei.com/en/support/bulletin/2021/10/	O-HUA-MAGI-201221/1220
IBM					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
aix					
Improper Privilege Management	09-Dec-21	2.1	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to gain privileges due to allowing modification of columns of existing tasks. IBM X-Force ID: 210321. **CVE ID : CVE-2021-38926**	https://exchange.xforce.ibmcloud.com/vulnerabilities/210321, https://www.ibm.com/support/pages/node/6523808	O-IBM-AIX-201221/1221
Exposure of Resource to Wrong Sphere	09-Dec-21	4	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1, and 11.5 is vulnerable to an information disclosure as a result of a connected user having indirect read access to a table where they are not authorized to select from. IBM X-Force ID: 210418. **CVE ID : CVE-2021-38931**	https://www.ibm.com/support/pages/node/6523810, https://exchange.xforce.ibmcloud.com/vulnerabilities/210418	O-IBM-AIX-201221/1222
Uncontrolled Resource Consumption	09-Dec-21	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available CPU resources. IBM X-Force ID: 211405. **CVE ID : CVE-2021-38951**	https://www.ibm.com/support/pages/node/6524674, https://exchange.xforce.ibmcloud.com/vulnerabilities/211405	O-IBM-AIX-201221/1223
Use of a Broken or Risky Cryptographic Algorithm	09-Dec-21	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 uses weaker than expected cryptographic algorithms that	https://exchange.xforce.ibmcloud.com/vulnerabilities/213217, https://ww	O-IBM-AIX-201221/1224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to decrypt highly sensitive information. **CVE ID : CVE-2021-39002**	w.ibm.com/support/pages/node/6523802	
Exposure of Resource to Wrong Sphere	09-Dec-21	5	IBM Db2 9.7, 10.1, 10.5, 11.1, and 11.5 may be vulnerable to an Information Disclosure when using the LOAD utility as under certain circumstances the LOAD utility does not enforce directory restrictions. IBM X-Force ID: 199521. **CVE ID : CVE-2021-20373**	https://www.ibm.com/support/pages/node/6523804, https://exchange.xforce.ibmcloud.com/vulnerabilities/195521	O-IBM-AIX-201221/1225
Incorrect Authorization	09-Dec-21	5.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a user with DBADM authority to access other databases and read or modify files. IBM X-Force ID: 199914. **CVE ID : CVE-2021-29678**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199914, https://www.ibm.com/support/pages/node/6523806	O-IBM-AIX-201221/1226
i					
Uncontrolled Resource Consumption	09-Dec-21	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available CPU resources. IBM X-Force ID: 211405. **CVE ID : CVE-2021-38951**	https://www.ibm.com/support/pages/node/6524674, https://exchange.xforce.ibmcloud.com/vulnerabilities/211405	O-IBM-I-201221/1227
powervm_hypervisor					
N/A	10-Dec-21	9.4	IBM PowerVM Hypervisor	https://exch	O-IBM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FW860, FW940, and FW950 could allow an attacker that gains service access to the FSP can read and write arbitrary host system memory through a series of carefully crafted service procedures. IBM X-Force ID: 210018. **CVE ID : CVE-2021-38917**	ange.xforce.ibmcloud.com/vulnerabilities/210018, https://www.ibm.com/support/pages/node/6525010	POWE-201221/1228
N/A	10-Dec-21	6.8	IBM PowerVM Hypervisor FW940, FW950, and FW1010 could allow an authenticated user to cause the system to crash using a specially crafted IBMi Hypervisor call. IBM X-Force ID: 210894. **CVE ID : CVE-2021-38937**	https://exchange.xforce.ibmcloud.com/vulnerabilities/210894, https://www.ibm.com/support/pages/node/6525014	O-IBM-POWE-201221/1229
z\\/os					
Uncontrolled Resource Consumption	09-Dec-21	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available CPU resources. IBM X-Force ID: 211405. **CVE ID : CVE-2021-38951**	https://www.ibm.com/support/pages/node/6524674, https://exchange.xforce.ibmcloud.com/vulnerabilities/211405	O-IBM-Z\\/-201221/1230
linaro					
op-tee					
Incorrect Permission Assignment for Critical	07-Dec-21	3.6	The OPTEE-OS CSU driver for NXP i.MX SoC devices lacks security access configuration for several models, resulting	N/A	O-LIN-OP-T-201221/1231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource			in TrustZone bypass because the NonSecure World can perform arbitrary memory read/write operations on Secure World memory. This involves a DMA capable peripheral. **CVE ID : CVE-2021-36133**		
Incorrect Authorization	07-Dec-21	4.6	An issue was discovered in Trusted Firmware OP-TEE Trusted OS through 3.15.0. The OPTEE-OS CSU driver for NXP i.MX6UL SoC devices lacks security access configuration for wakeup-related registers, resulting in TrustZone bypass because the NonSecure World can perform arbitrary memory read/write operations on Secure World memory. This involves a v cycle. **CVE ID : CVE-2021-44149**	https://github.com/f-secure-foundry/advisories/blob/master/Security_Advisory-Ref_FSC-HWSEC-VR2021-0002-OP-TEE_TrustZone_bypass_at_wakeup.txt	O-LIN-OP-T-201221/1232
Linux					
linux_kernel					
Improper Privilege Management	09-Dec-21	2.1	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to gain privileges due to allowing modification of columns of existing tasks. IBM X-Force ID: 210321. **CVE ID : CVE-2021-38926**	https://exchange.xforce.ibmcloud.com/vulnerabilities/210321, https://www.ibm.com/support/pages/node/6523808	O-LIN-LINU-201221/1233
Exposure of Resource to Wrong	09-Dec-21	4	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1, and	https://www.ibm.com/support/page	O-LIN-LINU-201221/1234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			11.5 is vulnerable to an information disclosure as a result of a connected user having indirect read access to a table where they are not authorized to select from. IBM X-Force ID: 210418. **CVE ID : CVE-2021-38931**	s/node/6523810, https://exchange.xforce.ibmcloud.com/vulnerabilities/210418	
Uncontrolled Resource Consumption	09-Dec-21	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available CPU resources. IBM X-Force ID: 211405. **CVE ID : CVE-2021-38951**	https://www.ibm.com/support/pages/node/6524674, https://exchange.xforce.ibmcloud.com/vulnerabilities/211405	O-LIN-LINU-201221/1235
Use of a Broken or Risky Cryptographic Algorithm	09-Dec-21	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID : CVE-2021-39002**	https://exchange.xforce.ibmcloud.com/vulnerabilities/213217, https://www.ibm.com/support/pages/node/6523802	O-LIN-LINU-201221/1236
Exposure of Resource to Wrong Sphere	09-Dec-21	5	IBM Db2 9.7, 10.1, 10.5, 11.1, and 11.5 may be vulnerable to an Information Disclosure when using the LOAD utility as under certain circumstances the LOAD utility does not enforce directory restrictions. IBM X-Force ID: 199521. **CVE ID : CVE-2021-20373**	https://www.ibm.com/support/pages/node/6523804, https://exchange.xforce.ibmcloud.com/vulnerabilities/195521	O-LIN-LINU-201221/1237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	01-Dec-21	5	IBM QRadar SIEM 7.3 and 7.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 196074. **CVE ID : CVE-2021-20400**	https://exchange.xforce.ibmcloud.com/vulnerabilities/196074, https://www.ibm.com/support/pages/node/6520488	O-LIN-LINU-201221/1238
Improper Privilege Management	01-Dec-21	9	The AMDPowerProfiler.sys driver of AMD ?Prof tool may allow lower privileged users to access MSRs in kernel which may lead to privilege escalation and ring-0 code execution by the lower privileged user. **CVE ID : CVE-2021-26334**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1016	O-LIN-LINU-201221/1239
Incorrect Authorization	09-Dec-21	5.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a user with DBADM authority to access other databases and read or modify files. IBM X-Force ID: 199914. **CVE ID : CVE-2021-29678**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199914, https://www.ibm.com/support/pages/node/6523806	O-LIN-LINU-201221/1240
Improper Authentication	01-Dec-21	4.3	IBM QRadar SIEM 7.3 and 7.4 could allow an attacker to obtain sensitive information due to the server performing key exchange without entity authentication on inter-host communications using man in the middle techniques. IBM X-Force ID: 203033. **CVE ID : CVE-2021-29779**	https://www.ibm.com/support/pages/node/6520484, https://exchange.xforce.ibmcloud.com/vulnerabilities/203033	O-LIN-LINU-201221/1241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-21	4.3	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 205281. **CVE ID : CVE-2021-29849**	https://www.ibm.com/support/pages/node/6520476, https://exchange.xforce.ibmcloud.com/vulnerabilities/205281	O-LIN-LINU-201221/1242
Server-Side Request Forgery (SSRF)	01-Dec-21	4	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to server side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. This vulnerability is due to an incomplete fix for CVE-2020-4786. IBM X-Force ID: 206087. **CVE ID : CVE-2021-29863**	https://exchange.xforce.ibmcloud.com/vulnerabilities/206087, https://www.ibm.com/support/pages/node/6520490	O-LIN-LINU-201221/1243
Microsoft					
windows					
Improper Privilege Management	06-Dec-21	6.8	When a user has admin rights in Serv-U Console, the user can move, create and delete any files are able to be accessed on the Serv-U host machine. **CVE ID : CVE-2021-35245**	https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_15-2-5_release_notes.htm,	O-MIC-WIND-201221/1244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.solarwinds.com/trust-center/security-advisories/CVE-2021-35245	
Improper Privilege Management	09-Dec-21	2.1	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to gain privileges due to allowing modification of columns of existing tasks. IBM X-Force ID: 210321. **CVE ID : CVE-2021-38926**	https://exchange.xforce.ibmcloud.com/vulnerabilities/210321, https://www.ibm.com/support/pages/node/6523808	O-MIC-WIND-201221/1245
Exposure of Resource to Wrong Sphere	09-Dec-21	4	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1, and 11.5 is vulnerable to an information disclosure as a result of a connected user having indirect read access to a table where they are not authorized to select from. IBM X-Force ID: 210418. **CVE ID : CVE-2021-38931**	https://www.ibm.com/support/pages/node/6523810, https://exchange.xforce.ibmcloud.com/vulnerabilities/210418	O-MIC-WIND-201221/1246
Uncontrolled Resource Consumption	09-Dec-21	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available CPU resources. IBM X-Force ID: 211405.	https://www.ibm.com/support/pages/node/6524674, https://exchange.xforce.ibmcloud.com/vulnerabilities/211405	O-MIC-WIND-201221/1247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-38951		
Use of a Broken or Risky Cryptographic Algorithm	09-Dec-21	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID : CVE-2021-39002**	https://exchange.xforce.ibmcloud.com/vulnerabilities/213217, https://www.ibm.com/support/pages/node/6523802	O-MIC-WIND-201221/1248
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Dec-21	6.9	An issue was discovered in Plex Media Server through 1.24.4.5081-e362dc1ee. An attacker (with a foothold in a endpoint via a low-privileged user account) can access the exposed RPC service of the update service component. This RPC functionality allows the attacker to interact with the RPC functionality and execute code from a path of his choice (local, or remote via SMB) because of a TOCTOU race condition. This code execution is in the context of the Plex update service (which runs as SYSTEM). **CVE ID : CVE-2021-42835**	https://forums.plex.tv/t/security-regarding-cve-2021-42835/761510, https://www.plex.tv/media-server-downloads/	O-MIC-WIND-201221/1249
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Dec-21	7.2	FlexiHub For Windows is affected by Buffer Overflow. IOCTL Handler 0x22001B in the FlexiHub For Windows above 2.0.4340 below 5.3.14268 allows local attackers to execute arbitrary code in kernel mode or cause	N/A	O-MIC-WIND-201221/1250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42990**		
Integer Overflow or Wraparound	07-Dec-21	7.2	FlexiHub For Windows is affected by Integer Overflow. IOCTL Handler 0x22001B in the FlexiHub For Windows above 2.0.4340 below 5.3.14268 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet. **CVE ID : CVE-2021-42993**	N/A	O-MIC-WIND-201221/1251
Files or Directories Accessible to External Parties	03-Dec-21	2.1	Trend Micro Security 2021 v17.0 (Consumer) contains a vulnerability that allows files inside the protected folder to be modified without any detection. **CVE ID : CVE-2021-43772**	https://helpcenter.trendmicro.com/en-us/article/tmka-10855	O-MIC-WIND-201221/1252
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Dec-21	4.3	Wiki.js is a wiki app built on Node.js. Prior to version 2.5.254, directory traversal outside of Wiki.js context is possible when a storage module with local asset cache fetching is enabled on a Windows host. A malicious user can potentially read any file on the file system by crafting a special URL that allows for directory traversal. This is only possible on a Wiki.js server running on	https://github.com/Requarks/wiki/commit/414033de9dff66a327e3f3243234852f468a9d85, https://github.com/Requarks/wiki/security/advisories/GHSA-r363-73gj-	O-MIC-WIND-201221/1253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows, when a storage module implementing local asset cache (e.g Local File System or Git) is enabled and that no web application firewall solution (e.g. cloudflare) strips potentially malicious URLs. Commit number 414033de9dff66a327e3f3243234852f468a9d85 fixes this vulnerability by sanitizing the path before it is passed on to the storage module. The sanitization step removes any windows directory traversal sequences from the path. As a workaround, disable any storage module with local asset caching capabilities (Local File System, Git). **CVE ID : CVE-2021-43800**	6j25	
Reachable Assertion	03-Dec-21	2.1	A reachable assertion vulnerability in Trend Micro Apex One could allow an attacker to crash the program on affected installations, leading to a denial-of-service (DoS). Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-44022**	https://success.trendmicro.com/solution/000289229	O-MIC-WIND-201221/1254
Out-of-bounds Read	07-Dec-21	4.3	Adobe Bridge versions 11.1.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive	https://helpx.adobe.com/security/products/bridge/apsb21-	O-MIC-WIND-201221/1255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious RGB file. **CVE ID : CVE-2021-44185**	94.html	
Out-of-bounds Read	07-Dec-21	4.3	Adobe Bridge versions 11.1.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious SGI file. **CVE ID : CVE-2021-44186**	https://helpx.adobe.com/security/products/bridge/apsb21-94.html	O-MIC-WIND-201221/1256
Out-of-bounds Read	07-Dec-21	4.3	Adobe Bridge versions 11.1.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious SGI file. **CVE ID : CVE-2021-44187**	https://helpx.adobe.com/security/products/bridge/apsb21-94.html	O-MIC-WIND-201221/1257
Exposure of Resource to	09-Dec-21	5	IBM Db2 9.7, 10.1, 10.5, 11.1, and 11.5 may be vulnerable	https://www.ibm.com/s	O-MIC-WIND-201221/1258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			to an Information Disclosure when using the LOAD utility as under certain circumstances the LOAD utility does not enforce directory restrictions. IBM X-Force ID: 199521. **CVE ID : CVE-2021-20373**	upport/pages/node/6523804, https://exchange.xforce.ibmcloud.com/vulnerabilities/195521	
Improper Privilege Management	01-Dec-21	9	The AMDPowerProfiler.sys driver of AMD ?Prof tool may allow lower privileged users to access MSRs in kernel which may lead to privilege escalation and ring-0 code execution by the lower privileged user. **CVE ID : CVE-2021-26334**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1016	O-MIC-WIND-201221/1259
Incorrect Authorization	09-Dec-21	5.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a user with DBADM authority to access other databases and read or modify files. IBM X-Force ID: 199914. **CVE ID : CVE-2021-29678**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199914, https://www.ibm.com/support/pages/node/6523806	O-MIC-WIND-201221/1260
Files or Directories Accessible to External Parties	08-Dec-21	5.5	A denial-of-service vulnerability in Database Security (DBS) prior to 4.8.4 allows a remote authenticated administrator to trigger a denial-of-service attack against the DBS server. The configuration of Archiving through the User interface incorrectly allowed the creation of directories and files in Windows system	https://kc.mcafee.com/corporate/index?page=content&id=SB10358	O-MIC-WIND-201221/1261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			directories and other locations where sensitive data could be overwritten. The former could lead to a DoS, whilst the latter could lead to data destruction on the DBS server. **CVE ID : CVE-2021-31850**		
windows_10					
Exposure of Resource to Wrong Sphere	08-Dec-21	4.3	Microsoft introduced a new feature in Windows 10 known as Cloud Clipboard which, if enabled, will record data copied to the clipboard to the cloud, and make it available on other computers in certain scenarios. Applications that wish to prevent copied data from being recorded in Cloud History must use specific clipboard formats; and Firefox before versions 94 and ESR 91.3 did not implement them. This could have caused sensitive data to be recorded to a user's Microsoft account. *This bug only affects Firefox for Windows 10+ with Cloud Clipboard enabled. Other operating systems are unaffected.*. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3. **CVE ID : CVE-2021-38505**	https://www.mozilla.org/security/advisories/mfsa2021-50/, https://www.mozilla.org/security/advisories/mfsa2021-49/, https://bugzilla.mozilla.org/show_bug.cgi?id=1730194, https://www.mozilla.org/security/advisories/mfsa2021-48/	O-MIC-WIND-201221/1262
windows_server_2012					
Improper	02-Dec-21	4	CA Network Flow Analysis	https://supp	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			(NFA) 21.2.1 and earlier contain a SQL injection vulnerability in the NFA web application, due to insufficient input validation, that could potentially allow an authenticated user to access sensitive data. **CVE ID : CVE-2021-44050**	ort.broadcom.com/external/content/security-advisories/CA20211201-01-Security-Notice-for-CA-Network-Flow-Analysis/19689	201221/1263
windows_server_2016					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-21	4	CA Network Flow Analysis (NFA) 21.2.1 and earlier contain a SQL injection vulnerability in the NFA web application, due to insufficient input validation, that could potentially allow an authenticated user to access sensitive data. **CVE ID : CVE-2021-44050**	https://support.broadcom.com/external/content/security-advisories/CA20211201-01-Security-Notice-for-CA-Network-Flow-Analysis/19689	O-MIC-WIND-201221/1264
windows_server_2019					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-21	4	CA Network Flow Analysis (NFA) 21.2.1 and earlier contain a SQL injection vulnerability in the NFA web application, due to insufficient input validation, that could potentially allow an authenticated user to access sensitive data. **CVE ID : CVE-2021-44050**	https://support.broadcom.com/external/content/security-advisories/CA20211201-01-Security-Notice-for-CA-Network-Flow-Analysis/196	O-MIC-WIND-201221/1265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				89	
mitsubishi					
melipc_mi5122-vw_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELI-201221/1266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELI-201221/1267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELI-201221/1268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r00_cpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20609		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r01_cpu_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper	01-Dec-21	7.8	Improper Input Validation	https://ww	O-MIT-MELS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All	w.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	201221/1274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r02_cpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency	https://www.mitsubishi	O-MIT-MELS-201221/1276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All	electric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r04_cpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series	https://www.mitsubishielectric.com/	O-MIT-MELS-201221/1278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series	en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and	https://www.mitsubishielectric.com/en/psirt/vul	O-MIT-MELS-201221/1280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series	nerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r04_pcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pd	O-MIT-MELS-201221/1282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series	f/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r08_cpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-	O-MIT-MELS-201221/1284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All	019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r08_pcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r08_sfcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r120_cpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r120_pcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r120_sfcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r12_ccpu-v_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r16_cpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r16_mtcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20609		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r16_pcpu_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper	01-Dec-21	7.8	Improper Input Validation	https://ww	O-MIT-MELS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All	w.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	201221/1313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r16_sfcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency	https://www.mitsubishi	O-MIT-MELS-201221/1315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All	electric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r32_cpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series	https://www.mitsubishielectric.com/	O-MIT-MELS-201221/1317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series	en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and	https://www.mitsubishielectric.com/en/psirt/vul	O-MIT-MELS-201221/1319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series	nerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r32_mtcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pd	O-MIT-MELS-201221/1321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series	f/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r32_pcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-	O-MIT-MELS-201221/1323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All	019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r32_sfcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_iq-r_r64_mtcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_l02cpu\\(-p\\)_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_l06cpu\\(-p\\)_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_l26cpu-\\(p\\)bt_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_l26cpu\\(-p\\)_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required for recovery. **CVE ID : CVE-2021-20611**		
melsec_mr-mq100_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q03udecpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20609		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q03udvcpu_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper	01-Dec-21	7.8	Improper Input Validation	https://ww	O-MIT-MELS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All	w.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	201221/1352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q04udecpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency	https://www.mitsubishi	O-MIT-MELS-201221/1354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All	electric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q04udpvcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series	https://www.mitsubishielectric.com/	O-MIT-MELS-201221/1356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series	en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and	https://www.mitsubishielectric.com/en/psirt/vul	O-MIT-MELS-201221/1358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series	nerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q04udvcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pd	O-MIT-MELS-201221/1360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series	f/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q06udecpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-	O-MIT-MELS-201221/1362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All	019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q06udpvcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q06udvcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q100udecpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q10udecpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q12dccpu-v_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q13udecpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q13udpvcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q13udvcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20609		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q170mcpu_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper	01-Dec-21	7.8	Improper Input Validation	https://ww	O-MIT-MELS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All	w.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	201221/1391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q170mscpu\\(-s1\\)_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency	https://www.mitsubishi	O-MIT-MELS-201221/1393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All	electric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q172dcpu-s1_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series	https://www.mitsubishielectric.com/	O-MIT-MELS-201221/1395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series	en/psirt/vulnerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and	https://www.mitsubishielectric.com/en/psirt/vul	O-MIT-MELS-201221/1397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series	nerability/pdf/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q172dscpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pd	O-MIT-MELS-201221/1399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series	f/2021-019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q173dcpu-s1_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-	O-MIT-MELS-201221/1401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All	019_en.pdf	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q173dscpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q20udecpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q24dhccpu-ls_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q24dhccpu-v\\(g\\)_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q26dhccpu-ls_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q26udecpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q26udpvcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q26udvcpu_firmware					
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20609		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper Input Validation	01-Dec-21	7.8	Improper Input Validation vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
melsec_q50udecpu_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	01-Dec-21	7.8	Uncontrolled Resource Consumption vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20609**		
N/A	01-Dec-21	7.8	Improper Handling of Length Parameter Inconsistency vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	O-MIT-MELS-201221/1429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20610**		
Improper	01-Dec-21	7.8	Improper Input Validation	https://ww	O-MIT-MELS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability in MELSEC iQ-R Series R00/01/02CPU Firmware versions "24" and prior, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "57" and prior, MELSEC iQ-R Series R08/16/32/120SFCPU All versions, MELSEC iQ-R Series R08/16/32/120PCPU Firmware versions "29" and prior, MELSEC iQ-R Series R08/16/32/120PSFCPU All versions, MELSEC iQ-R Series R16/32/64MTCPU All versions, MELSEC iQ-R Series R12CCPU-V All versions, MELSEC Q Series Q03UDECPU All versions, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU All versions, MELSEC Q Series Q03/04/06/13/26UDVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q04/06/13/26UDPVCPU The first 5 digits of serial No. "23071" and prior, MELSEC Q Series Q12DCCPU-V All versions, MELSEC Q Series Q24DHCCPU-V(G) All versions, MELSEC Q Series Q24/26DHCCPU-LS All versions, MELSEC Q Series MR-MQ100 All versions, MELSEC Q Series Q172/173DCPU-S1 All versions, MELSEC Q Series Q172/172DSCPU All	w.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-019_en.pdf	201221/1430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, MELSEC Q Series Q170MCPU All versions, MELSEC Q Series Q170MSCPU(-S1) All versions, MELSEC L Series L02/06/26CPU(-P) All versions, MELSEC L Series L26CPU-(P)BT All versions and MELIPC Series MI5122-VW All versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery. **CVE ID : CVE-2021-20611**		
Netgear					
rax35_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Dec-21	3.6	A path traversal attack in web interfaces of Netgear RAX35, RAX38, and RAX40 routers before v1.0.4.102, allows a remote unauthenticated attacker to gain access to sensitive restricted information, such as forbidden files of the web application, via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41449**	http://netgear.com, https://kb.netgear.com/000064405/Security-Advisory-for-Path-Traversal-on-Some-Routers-PSV-2021-0268, https://www.netgear.com/about/security/	O-NET-RAX3-201221/1431
rax38_firmware					
Improper Limitation of a Pathname	09-Dec-21	3.6	A path traversal attack in web interfaces of Netgear RAX35, RAX38, and RAX40 routers	http://netgear.com, https://kb.n	O-NET-RAX3-201221/1432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			before v1.0.4.102, allows a remote unauthenticated attacker to gain access to sensitive restricted information, such as forbidden files of the web application, via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41449**	etgear.com/000064405/Security-Advisory-for-Path-Traversal-on-Some-Routers-PSV-2021-0268, https://www.netgear.com/about/security/	
rax40_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Dec-21	3.6	A path traversal attack in web interfaces of Netgear RAX35, RAX38, and RAX40 routers before v1.0.4.102, allows a remote unauthenticated attacker to gain access to sensitive restricted information, such as forbidden files of the web application, via sending a specially crafted HTTP packet. **CVE ID : CVE-2021-41449**	http://netgear.com, https://kb.netgear.com/000064405/Security-Advisory-for-Path-Traversal-on-Some-Routers-PSV-2021-0268, https://www.netgear.com/about/security/	O-NET-RAX4-201221/1433
Nttdocomo					
wi-fi_station_sh-52a_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site	01-Dec-21	4.3	Cross-site scripting vulnerability in Wi-Fi STATION SH-52A (38JP_1_11G, 38JP_1_11J, 38JP_1_11K, 38JP_1_11L, 38JP_1_26F, 38JP_1_26G, 38JP_1_26J, 38JP_2_03B, and	N/A	O-NTT-WI-F-201221/1434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			38JP_2_03C) allows a remote unauthenticated attacker to inject an arbitrary script via WebUI of the device. **CVE ID : CVE-2021-20847**		
nxp					
kinetis_k82_firmware					
Out-of-bounds Read	01-Dec-21	2.1	NXP Kinetis K82 devices have a buffer over-read via a crafted wlength value in a GET Status-Other request during use of USB In-System Programming (ISP) mode. This discloses protected flash memory. **CVE ID : CVE-2021-44479**	N/A	O-NXP-KINE-201221/1435
lpc55s69jbd100_firmware					
Out-of-bounds Read	01-Dec-21	2.1	NXP LPC55S69 devices before A3 have a buffer over-read via a crafted wlength value in a GET Descriptor Configuration request during use of USB In-System Programming (ISP) mode. This discloses protected flash memory. **CVE ID : CVE-2021-40154**	N/A	O-NXP-LPC5-201221/1436
lpc55s69jbd64_firmware					
Out-of-bounds Read	01-Dec-21	2.1	NXP LPC55S69 devices before A3 have a buffer over-read via a crafted wlength value in a GET Descriptor Configuration request during use of USB In-System Programming (ISP) mode. This discloses protected flash memory.	N/A	O-NXP-LPC5-201221/1437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40154		
lpc55s69jev98_firmware					
Out-of-bounds Read	01-Dec-21	2.1	NXP LPC55S69 devices before A3 have a buffer over-read via a crafted wlength value in a GET Descriptor Configuration request during use of USB In-System Programming (ISP) mode. This discloses protected flash memory. **CVE ID : CVE-2021-40154**	N/A	O-NXP-LPC5-201221/1438
lpc55s69_firmware					
Out-of-bounds Read	01-Dec-21	2.1	NXP Kinetis K82 devices have a buffer over-read via a crafted wlength value in a GET Status-Other request during use of USB In-System Programming (ISP) mode. This discloses protected flash memory. **CVE ID : CVE-2021-44479**	N/A	O-NXP-LPC5-201221/1439
Oracle					
solaris					
Improper Privilege Management	09-Dec-21	2.1	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to gain privileges due to allowing modification of columns of existing tasks. IBM X-Force ID: 210321. **CVE ID : CVE-2021-38926**	https://exchange.xforce.ibmcloud.com/vulnerabilities/210321, https://www.ibm.com/support/pages/node/6523808	O-ORA-SOLA-201221/1440
Exposure of Resource to Wrong	09-Dec-21	4	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1, and	https://www.ibm.com/support/page	O-ORA-SOLA-201221/1441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			11.5 is vulnerable to an information disclosure as a result of a connected user having indirect read access to a table where they are not authorized to select from. IBM X-Force ID: 210418. **CVE ID : CVE-2021-38931**	s/node/6523810, https://exchange.xforce.ibmcloud.com/vulnerabilities/210418	
Uncontrolled Resource Consumption	09-Dec-21	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available CPU resources. IBM X-Force ID: 211405. **CVE ID : CVE-2021-38951**	https://www.ibm.com/support/pages/node/6524674, https://exchange.xforce.ibmcloud.com/vulnerabilities/211405	O-ORA-SOLA-201221/1442
Use of a Broken or Risky Cryptographic Algorithm	09-Dec-21	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID : CVE-2021-39002**	https://exchange.xforce.ibmcloud.com/vulnerabilities/213217, https://www.ibm.com/support/pages/node/6523802	O-ORA-SOLA-201221/1443
Exposure of Resource to Wrong Sphere	09-Dec-21	5	IBM Db2 9.7, 10.1, 10.5, 11.1, and 11.5 may be vulnerable to an Information Disclosure when using the LOAD utility as under certain circumstances the LOAD utility does not enforce directory restrictions. IBM X-Force ID: 199521. **CVE ID : CVE-2021-20373**	https://www.ibm.com/support/pages/node/6523804, https://exchange.xforce.ibmcloud.com/vulnerabilities/195521	O-ORA-SOLA-201221/1444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	09-Dec-21	5.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a user with DBADM authority to access other databases and read or modify files. IBM X-Force ID: 199914. **CVE ID : CVE-2021-29678**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199914, https://www.ibm.com/support/pages/node/6523806	O-ORA-SOLA-201221/1445
raspberrypi					
raspberry_pi_os_lite					
Improper Privilege Management	07-Dec-21	10	Raspberry Pi OS through 5.10 has the raspberry default password for the pi account. If not changed, attackers can gain administrator privileges. **CVE ID : CVE-2021-38759**	https://www.raspberrypi.com/documentation/computers/configuration.html#change-the-default-password	O-RAS-RASP-201221/1446
Redhat					
enterprise_linux					
Out-of-bounds Read	08-Dec-21	6.4	An out-of-bounds read flaw was found in the CLARRV, DLARRV, SLARRV, and ZLARRV functions in lapack through version 3.10.0, as also used in OpenBLAS before version 0.3.18. Specially crafted inputs passed to these functions could cause an application using lapack to crash or possibly disclose portions of its memory. **CVE ID : CVE-2021-4048**	https://github.com/JuliaLang/julia/issues/42415, https://github.com/xianyi/OpenBLAS/commit/337b65133df174796794871b3988cd03426e6d41, https://github.com/xianyi/OpenBLAS/commit/2be	O-RED-ENTE-201221/1447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				5ee3cca97a597f2ee2118808a2d5eacea050c	
satellite					
Improper Authentication	08-Dec-21	7.5	In Django 2.2 before 2.2.25, 3.1 before 3.1.14, and 3.2 before 3.2.10, HTTP requests for URLs with trailing newlines could bypass upstream access control based on URL paths. **CVE ID : CVE-2021-44420**	https://docs.djangoproject.com/en/3.2/releases/security/, https://www.openwall.com/lists/oss-security/2021/12/07/1, https://www.djangoproject.com/weblog/2021/dec/07/security-releases/	O-RED-SATE-201221/1448
renesas					
rx65n_firmware					
Insufficiently Protected Credentials	02-Dec-21	2.1	An issue was discovered on Renesas RX65 and RX65N devices. With a VCC glitch, an attacker can extract the security ID key from the device. Then, the protected firmware can be extracted. **CVE ID : CVE-2021-43327**	N/A	O-REN-RX65-201221/1449
rx65_firmware					
Insufficiently Protected Credentials	02-Dec-21	2.1	An issue was discovered on Renesas RX65 and RX65N devices. With a VCC glitch, an attacker can extract the security ID key from the	N/A	O-REN-RX65-201221/1450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Then, the protected firmware can be extracted. **CVE ID : CVE-2021-43327**		
solardatasystems					
solar-log_500_firmware					
Missing Authorization	07-Dec-21	5	The web administration server in Solar-Log 500 before 2.8.2 Build 52 does not require authentication, which allows remote attackers to gain administrative privileges by connecting to the server. As a result, the attacker can modify configuration files and change the system status. **CVE ID : CVE-2021-34543**	https://www.solar-log.com/en/support/firmware/	O-SOL-SOLA-201221/1451
Sonicwall					
sma_200_firmware					
Out-of-bounds Write	08-Dec-21	7.5	A Stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod_cgi module environment variables allows a remote unauthenticated attacker to potentially execute code as a 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions. **CVE ID : CVE-2021-20038**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1452
Improper Neutralization of Special Elements used in an OS	08-Dec-21	9	Improper neutralization of special elements in the SMA100 management interface '/cgi-bin/viewcert' POST http method allows a	https://psirt.global.sonicwall.com/vuln-detail/SNWL	O-SON-SMA_-201221/1453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			remote authenticated attacker to inject arbitrary commands as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20039**	ID-2021-0026	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-21	5	A relative path traversal vulnerability in the SMA100 upload funtion allows a remote unauthenticated attacker to upload crafted web pages or files as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20040**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1454
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Dec-21	7.8	An unauthenticated and remote adversary can consume all of the device's CPU due to crafted HTTP requests sent to SMA100 /fileshare/sonicfiles/sonicfiles resulting in a loop with unreachable exit condition. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20041**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1455
Externally Controlled Reference to a Resource in Another Sphere	08-Dec-21	7.5	An unauthenticated remote attacker can use SMA 100 as an unintended proxy or intermediary undetectable proxy to bypass firewall rules. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20042**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Dec-21	6.5	A Heap-based buffer overflow vulnerability in SonicWall SMA100 getBookmarks method allows a remote authenticated attacker to potentially execute code as the nobody user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20043**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1457
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	A post-authentication remote command injection vulnerability in SonicWall SMA100 allows a remote authenticated attacker to execute OS system commands in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20044**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1458
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	7.5	A buffer overflow vulnerability in SMA100 sonicfiles RAC_COPY_TO (RacNumber 36) method allows a remote unauthenticated attacker to potentially execute code as the 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20045**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1459
sma_210_firmware					
Out-of-bounds Write	08-Dec-21	7.5	A Stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod_cgi module	https://psirt.global.sonicwall.com/vuln-	O-SON-SMA_-201221/1460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			environment variables allows a remote unauthenticated attacker to potentially execute code as a 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions. **CVE ID : CVE-2021-20038**	detail/SNWLID-2021-0026	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	Improper neutralization of special elements in the SMA100 management interface '/cgi-bin/viewcert' POST http method allows a remote authenticated attacker to inject arbitrary commands as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20039**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1461
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-21	5	A relative path traversal vulnerability in the SMA100 upload funtion allows a remote unauthenticated attacker to upload crafted web pages or files as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20040**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1462
Loop with Unreachable Exit Condition ('Infinite	08-Dec-21	7.8	An unauthenticated and remote adversary can consume all of the device's CPU due to crafted HTTP requests sent to SMA100	https://psirt.global.sonicwall.com/vuln-detail/SNWL	O-SON-SMA_-201221/1463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop')			/fileshare/sonicfiles/sonicfiles resulting in a loop with unreachable exit condition. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20041**	ID-2021-0026	
Externally Controlled Reference to a Resource in Another Sphere	08-Dec-21	7.5	An unauthenticated remote attacker can use SMA 100 as an unintended proxy or intermediary undetectable proxy to bypass firewall rules. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20042**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1464
Out-of-bounds Write	08-Dec-21	6.5	A Heap-based buffer overflow vulnerability in SonicWall SMA100 getBookmarks method allows a remote authenticated attacker to potentially execute code as the nobody user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20043**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1465
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	A post-authentication remote command injection vulnerability in SonicWall SMA100 allows a remote authenticated attacker to execute OS system commands in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20044**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	7.5	A buffer overflow vulnerability in SMA100 sonicfiles RAC_COPY_TO (RacNumber 36) method allows a remote unauthenticated attacker to potentially execute code as the 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20045**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1467
sma_400_firmware					
Out-of-bounds Write	08-Dec-21	7.5	A Stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod_cgi module environment variables allows a remote unauthenticated attacker to potentially execute code as a 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions. **CVE ID : CVE-2021-20038**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1468
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	Improper neutralization of special elements in the SMA100 management interface '/cgi-bin/viewcert' POST http method allows a remote authenticated attacker to inject arbitrary commands as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20039		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-21	5	A relative path traversal vulnerability in the SMA100 upload funtion allows a remote unauthenticated attacker to upload crafted web pages or files as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20040**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1470
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Dec-21	7.8	An unauthenticated and remote adversary can consume all of the device's CPU due to crafted HTTP requests sent to SMA100 /fileshare/sonicfiles/sonicfiles resulting in a loop with unreachable exit condition. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20041**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1471
Externally Controlled Reference to a Resource in Another Sphere	08-Dec-21	7.5	An unauthenticated remote attacker can use SMA 100 as an unintended proxy or intermediary undetectable proxy to bypass firewall rules. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20042**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1472
Out-of-bounds Write	08-Dec-21	6.5	A Heap-based buffer overflow vulnerability in SonicWall SMA100 getBookmarks method allows a remote authenticated attacker to potentially execute code as	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-	O-SON-SMA_-201221/1473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the nobody user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20043**	0026	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	A post-authentication remote command injection vulnerability in SonicWall SMA100 allows a remote authenticated attacker to execute OS system commands in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20044**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1474
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	7.5	A buffer overflow vulnerability in SMA100 sonicfiles RAC_COPY_TO (RacNumber 36) method allows a remote unauthenticated attacker to potentially execute code as the 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20045**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1475
sma_410_firmware					
Out-of-bounds Write	08-Dec-21	7.5	A Stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod_cgi module environment variables allows a remote unauthenticated attacker to potentially execute code as a 'nobody' user in the appliance. This vulnerability affected SMA	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions. **CVE ID : CVE-2021-20038**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	Improper neutralization of special elements in the SMA100 management interface '/cgi-bin/viewcert' POST http method allows a remote authenticated attacker to inject arbitrary commands as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20039**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1477
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-21	5	A relative path traversal vulnerability in the SMA100 upload funtion allows a remote unauthenticated attacker to upload crafted web pages or files as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20040**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1478
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Dec-21	7.8	An unauthenticated and remote adversary can consume all of the device's CPU due to crafted HTTP requests sent to SMA100 /fileshare/sonicfiles/sonicfiles resulting in a loop with unreachable exit condition. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20041		
Externally Controlled Reference to a Resource in Another Sphere	08-Dec-21	7.5	An unauthenticated remote attacker can use SMA 100 as an unintended proxy or intermediary undetectable proxy to bypass firewall rules. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20042**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1480
Out-of-bounds Write	08-Dec-21	6.5	A Heap-based buffer overflow vulnerability in SonicWall SMA100 getBookmarks method allows a remote authenticated attacker to potentially execute code as the nobody user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20043**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1481
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	A post-authentication remote command injection vulnerability in SonicWall SMA100 allows a remote authenticated attacker to execute OS system commands in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20044**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1482
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	7.5	A buffer overflow vulnerability in SMA100 sonicfiles RAC_COPY_TO (RacNumber 36) method allows a remote unauthenticated attacker to potentially execute code as	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1483

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20045**		
sma_500v_firmware					
Out-of-bounds Write	08-Dec-21	7.5	A Stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod_cgi module environment variables allows a remote unauthenticated attacker to potentially execute code as a 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions. **CVE ID : CVE-2021-20038**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1484
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-21	9	Improper neutralization of special elements in the SMA100 management interface '/cgi-bin/viewcert' POST http method allows a remote authenticated attacker to inject arbitrary commands as a 'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20039**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1485
Improper Limitation of a Pathname to a Restricted Directory	08-Dec-21	5	A relative path traversal vulnerability in the SMA100 upload funtion allows a remote unauthenticated attacker to upload crafted web pages or files as a	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-	O-SON-SMA_-201221/1486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			'nobody' user. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20040**	0026	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Dec-21	7.8	An unauthenticated and remote adversary can consume all of the device's CPU due to crafted HTTP requests sent to SMA100 /fileshare/sonicfiles/sonicfiles resulting in a loop with unreachable exit condition. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20041**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1487
Externally Controlled Reference to a Resource in Another Sphere	08-Dec-21	7.5	An unauthenticated remote attacker can use SMA 100 as an unintended proxy or intermediary undetectable proxy to bypass firewall rules. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20042**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1488
Out-of-bounds Write	08-Dec-21	6.5	A Heap-based buffer overflow vulnerability in SonicWall SMA100 getBookmarks method allows a remote authenticated attacker to potentially execute code as the nobody user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20043**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1489
Improper Neutralizatio	08-Dec-21	9	A post-authentication remote command injection	https://psirt.global.sonic	O-SON-SMA_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			vulnerability in SonicWall SMA100 allows a remote authenticated attacker to execute OS system commands in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20044**	wall.com/vuln-detail/SNWLID-2021-0026	201221/1490
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-21	7.5	A buffer overflow vulnerability in SMA100 sonicfiles RAC_COPY_TO (RacNumber 36) method allows a remote unauthenticated attacker to potentially execute code as the 'nobody' user in the appliance. This vulnerability affected SMA 200, 210, 400, 410 and 500v appliances. **CVE ID : CVE-2021-20045**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026	O-SON-SMA_-201221/1491
Tendacn					
ac15_firmware					
Out-of-bounds Write	03-Dec-21	7.5	A Stack-based Buffer Overflow vulnerability exists in the Tenda AC15 V15.03.05.18_multi device via the list parameter in a post request in goform/SetIpMacBind. **CVE ID : CVE-2021-44352**	N/A	O-TEN-AC15-201221/1492
Tp-link					
archer_ax10_firmware					
Exposure of Resource to Wrong Sphere	07-Dec-21	7.8	A denial-of-service attack in WPA2, and WPA3-SAE authentication methods in TP-Link AX10v1 before V1_211014, allows a remote	https://www.tp-link.com/us/support/download/archer	O-TP--ARCH-201221/1493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to disconnect an already connected wireless client via sending with a wireless adapter specific spoofed authentication frames **CVE ID : CVE-2021-40288**	-ax10/v1/#Firmware	
archer_ax10_v1_firmware					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	08-Dec-21	5	An HTTP request smuggling attack in TP-Link AX10v1 before v1_211117 allows a remote unauthenticated attacker to DoS the web application via sending a specific HTTP packet. **CVE ID : CVE-2021-41450**	https://www.tp-link.com/us/support/download/archer-ax10/v1/#Firmware, http://tp-link.com	O-TP--ARCH-201221/1494
ui					
unifi_switch_firmware					
Uncontrolled Resource Consumption	07-Dec-21	6.1	A vulnerability found in UniFi Switch firmware Version 5.43.35 and earlier allows a malicious actor who has already gained access to the network to perform a Deny of Service (DoS) attack on the affected switch.This vulnerability is fixed in UniFi Switch firmware 5.76.6 and later. **CVE ID : CVE-2021-44527**	https://community.ui.com/releases/Security-Advisory-Bulletin-022-022/cd83c01b-33e4-454a-b3b9-1c3ccebea7cb	O-UI-UNIF-201221/1495
vinga					
wr-n300u_firmware					
Improper Neutralization of Special Elements	06-Dec-21	6.5	VINGA WR-N300U 77.102.1.4853 is affected by a command execution vulnerability in the goahead	N/A	O-VIN-WR-N-201221/1496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			component. **CVE ID : CVE-2021-43469**		
webhmi					
webhmi_firmware					
Improper Authenticati on	06-Dec-21	7.5	The authentication algorithm of the WebHMI portal is sound, but the implemented mechanism can be bypassed as the result of a separate weakness that is primary to the authentication error. **CVE ID : CVE-2021-43931**	https://us-cert.cisa.gov/ics/advisories/icsa-21-336-03	O-WEB-WEBH-201221/1497
Unrestricted Upload of File with Dangerous Type	06-Dec-21	10	The software allows the attacker to upload or transfer files of dangerous types to the WebHMI portal, that may be automatically processed within the product's environment or lead to arbitrary code execution. **CVE ID : CVE-2021-43936**	https://us-cert.cisa.gov/ics/advisories/icsa-21-336-03	O-WEB-WEBH-201221/1498
wokkalokka					
wokka_watch_q50_firmware					
Missing Encryption of Sensitive Data	01-Dec-21	9.3	Wokka Lokka Q50 devices through 2021-11-30 allow remote attackers (who know the SIM phone number and password) to listen to a device's surroundings via a callback in an SMS command, as demonstrated by the 123456 and 523681 default passwords. **CVE ID : CVE-2021-44480**	N/A	O-WOK-WOKK-201221/1499
XEN					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xen					
N/A	07-Dec-21	6.9	grant table v2 status pages may remain accessible after de-allocation (take two) Guest get permitted access to certain Xen-owned pages of memory. The majority of such pages remain allocated / associated with a guest for its entire lifetime. Grant table v2 status pages, however, get de-allocated when a guest switched (back) from v2 to v1. The freeing of such pages requires that the hypervisor know where in the guest these pages were mapped. The hypervisor tracks only one use within guest space, but racing requests from the guest to insert mappings of these pages may result in any of them to become mapped in multiple locations. Upon switching back from v2 to v1, the guest would then retain access to a page that was freed and perhaps re-used for other purposes. This bug was fortuitously fixed by code cleanup in Xen 4.14, and backported to security-supported Xen branches as a prerequisite of the fix for XSA-378. **CVE ID : CVE-2021-28703**	https://xenbits.xenproject.org/xsa/advisory-387.txt	O-XEN-XEN-201221/1500