https://nciipc.gov.in/

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Nov 2021 **Vol. 08 No. 21**

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
404_to_301_project					
404_to_301					
Cross-Site Request Forgery (CSRF)	08-Nov-21	4.3	The 404 to 301 â€“ Redirect, Log and Notify 404 Errors WordPress plugin before 3.0.9 does not have CSRF check in place when cleaning the logs, which could allow attacker to make a logged in admin delete all of them via a CSRF attack **CVE ID : CVE-2021-24766**	N/A	A-404-404_-181121/1
addtoany					
addtoany_share_buttons					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	3.5	The AddToAny Share Buttons WordPress plugin before 1.7.48 does not escape its Image URL button setting, which could lead allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24616**	https://plugins.trac.wordpress.org/changeset/2609928/	A-ADD-ADDT-181121/2
akka					
http_server					
Out-of-bounds Write	02-Nov-21	5	Akka HTTP 10.1.x and 10.2.x before 10.2.7 can encounter stack exhaustion while parsing HTTP	https://doc.akka.io/docs/akka-http/current	A-AKK-HTTP-181121/3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			headers, which allows a remote attacker to conduct a Denial of Service attack by sending a User-Agent header with deeply nested comments. **CVE ID : CVE-2021-42697**	/security/2021-CVE-2021-42697-stack-overflow-parsing-user-agent.html, https://akka.io/blog/, https://akka.io/blog/news/2021/11/02/akka-http-10.2.7-released	
Alibaba					
druid					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Nov-21	5	In Druid 1.2.3, visiting the path with parameter in a certain function can lead to directory traversal. **CVE ID : CVE-2021-33800**	https://security.alibaba.com/announcement/announcement?id=214	A-ALI-DRUI-181121/4
androidbubbles					
wp_header_images					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	4.3	The WP Header Images WordPress plugin before 2.0.1 does not sanitise and escape the t parameter before outputting it back in the plugin's settings page, leading to a Reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24798**	N/A	A-AND-WP_H-181121/5

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
antennahouse					
office_server_document_converter					
Improper Restriction of XML External Entity Reference	01-Nov-21	5	Office Server Document Converter V7.2MR4 and earlier and V7.1MR7 and earlier allows a remote unauthenticated attacker to conduct an XML External Entity (XXE) attack to cause a denial of service (DoS) condition by processing a specially crafted XML document. **CVE ID : CVE-2021-20838**	https://www.antenna.co.jp/news/2021/osdc72-20211027.html	A-ANT-OFFI-181121/6
Improper Restriction of XML External Entity Reference	01-Nov-21	4.3	Office Server Document Converter V7.2MR4 and earlier and V7.1MR7 and earlier allows a remote unauthenticated attacker to conduct an XML External Entity (XXE) attack to cause a denial of service (DoS) condition to the other servers by processing a specially crafted XML document. **CVE ID : CVE-2021-20839**	https://www.antenna.co.jp/news/2021/osdc72-20211027.html	A-ANT-OFFI-181121/7
Apache					
dolphinscheduler					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-21	6	In Apache DolphinScheduler before 1.3.6 versions, authorized users can use SQL injection in the data source center. (Only applicable to MySQL data source with internal login account password) **CVE ID : CVE-2021-27644**	https://lists.apache.org/thread.html/r35d6acf021486a390a7ea09e6650c2fe19e72522bd484791d606a6e6%40%	A-APA-DOLP-181121/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				3Cdev.dolphinscheduler.apache.org%3E	
mina					
Loop with Unreachable Exit Condition ('Infinite Loop')	01-Nov-21	4.3	In Apache MINA, a specifically crafted, malformed HTTP request may cause the HTTP Header decoder to loop indefinitely. The decoder assumed that the HTTP Header begins at the beginning of the buffer and loops if there is more data than expected. Please update MINA to 2.1.5 or greater. **CVE ID : CVE-2021-41973**	https://lists.apache.org/thread.html/r0b907da9340d5ff4e6c1a4798ef4e79700a668657f27cca8a39e9250%40%3Cdev.mina.apache.org%3E, http://www.openwall.com/lists/oss-security/2021/11/01/2	A-APA-MINA-181121/9
traffic_server					
Improper Input Validation	03-Nov-21	5	Improper input validation vulnerability in header parsing of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 8.1.2 and 9.0.0 to 9.1.0. **CVE ID : CVE-2021-37147**	https://lists.apache.org/thread/k01797hyncx53659wr3o72s5cvkc3164	A-APA-TRAF-181121/10
Improper Input Validation	03-Nov-21	5	Improper input validation vulnerability in header parsing of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 8.1.2 and	https://lists.apache.org/thread/k01797hyncx53659wr3o72s5cvkc3164	A-APA-TRAF-181121/11

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
			9.0.0 to 9.0.1. **CVE ID : CVE-2021-37148**		
Improper Input Validation	03-Nov-21	5	Improper Input Validation vulnerability in header parsing of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 8.1.2 and 9.0.0 to 9.1.0. **CVE ID : CVE-2021-37149**	https://lists.apache.org/thread/k01797hyncx53659wr3o72s5cvkc3164	A-APA-TRAF-181121/12
Improper Authentication	03-Nov-21	6.8	Improper Authentication vulnerability in TLS origin verification of Apache Traffic Server allows for man in the middle attacks. This issue affects Apache Traffic Server 8.0.0 to 8.0.8. **CVE ID : CVE-2021-38161**	https://lists.apache.org/thread/k01797hyncx53659wr3o72s5cvkc3164	A-APA-TRAF-181121/13
Improper Input Validation	03-Nov-21	5	Improper Input Validation vulnerability in accepting socket connections in Apache Traffic Server allows an attacker to make the server stop accepting new connections. This issue affects Apache Traffic Server 5.0.0 to 9.1.0. **CVE ID : CVE-2021-41585**	https://lists.apache.org/thread/k01797hyncx53659wr3o72s5cvkc3164	A-APA-TRAF-181121/14
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Nov-21	7.5	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in the stats-over-http plugin of Apache Traffic Server allows an attacker to overwrite memory. This issue affects Apache Traffic Server 9.1.0.	https://lists.apache.org/thread/k01797hyncx53659wr3o72s5cvkc3164	A-APA-TRAF-181121/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-43082		
apostrophecms					
apostrophecms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Nov-21	3.5	Apostrophe CMS versions between 2.63.0 to 3.3.1 are vulnerable to Stored XSS where an editor uploads an SVG file that contains malicious JavaScript onto the Images module, which triggers XSS once viewed. **CVE ID : CVE-2021-25978**	https://github.com/apostrophecms/apostrophe/commit/c8b94ee9c79468f1ce28e31966cb0e0839165e59	A-APO-APOS-181121/16
Insufficient Session Expiration	08-Nov-21	6.4	Apostrophe CMS versions between 2.63.0 to 3.3.1 affected by an insufficient session expiration vulnerability, which allows unauthenticated remote attackers to hijack recently logged-in users' sessions. **CVE ID : CVE-2021-25979**	https://github.com/apostrophecms/apostrophe/commit/c211b211f9f4303a77a307cf41aac9b4ef8d2c7c	A-APO-APOS-181121/17
Artica					
pandora_fms					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Nov-21	4.6	With an admin account, the .htaccess file in Artica Pandora FMS <=755 can be overwritten with the File Manager component. The new .htaccess file contains a Rewrite Rule with a type definition. A normal PHP file can be uploaded with this new "file type" and the code can be executed with an HTTP request. **CVE ID : CVE-2021-36697**	http://artica.com, http://pandora.com	A-ART-PAND-181121/18
Improper	03-Nov-21	3.5	Pandora FMS through 755	http://artica	A-ART-PAND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			allows XSS via a new Event Filter with a crafted name. **CVE ID : CVE-2021-36698**	.com, http://pandora.com	181121/19
asgaros					
asgaros_forum					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	7.5	The Asgaros Forum WordPress plugin before 1.15.13 does not validate and escape user input when subscribing to a topic before using it in a SQL statement, leading to an unauthenticated SQL injection issue **CVE ID : CVE-2021-24827**	https://plugins.trac.wordpress.org/changeset/2611560/asgaros-forum	A-ASG-ASGA-181121/20
Atlassian					
data_center					
Improper Authentication	03-Nov-21	5	Affected versions of Atlassian Jira Server and Data Center allow a remote attacker who has had their access revoked from Jira Service Management to enable and disable Issue Collectors on Jira Service Management projects via an Improper Authentication vulnerability in the /secure/ViewCollectors endpoint. The affected versions are before version 8.19.1. **CVE ID : CVE-2021-41312**	https://jira.atlassian.com/browse/JRASERVER-72801	A-ATL-DATA-181121/21
jira					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	03-Nov-21	5	Affected versions of Atlassian Jira Server and Data Center allow a remote attacker who has had their access revoked from Jira Service Management to enable and disable Issue Collectors on Jira Service Management projects via an Improper Authentication vulnerability in the /secure/ViewCollectors endpoint. The affected versions are before version 8.19.1. **CVE ID : CVE-2021-41312**	https://jira.atlassian.com/browse/JRASERVER-72801	A-ATL-JIRA-181121/22
jira_software_data_center					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	4.3	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in the Associated Projects feature (/secure/admin/AssociatedProjectsForCustomField.jspa). The affected versions are before version 8.5.19, from version 8.6.0 before 8.13.11, and from version 8.14.0 before 8.19.1. **CVE ID : CVE-2021-41310**	https://jira.atlassian.com/browse/JRASERVER-72800	A-ATL-JIRA-181121/23
Missing Authorization	01-Nov-21	4	Affected versions of Atlassian Jira Server and Data Center allow authenticated but non-admin remote attackers to	https://jira.atlassian.com/browse/JRASERVER-72898	A-ATL-JIRA-181121/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			edit email batch configurations via an Improper Authorization vulnerability in the /secure/admin/ConfigureBatching!default.jspa endpoint. The affected versions are before version 8.21.0. **CVE ID : CVE-2021-41313**		
automatorwp					
automatorwp					
Incorrect Authorization	01-Nov-21	6.5	The AutomatorWP WordPress plugin before 1.7.6 does not perform capability checks which allows users with Subscriber roles to enumerate automations, disclose title of private posts or user emails, call functions, or perform privilege escalation via Ajax actions. **CVE ID : CVE-2021-24717**	N/A	A-AUT-AUTO-181121/25
Azeotech					
daqfactory					
Use of Inherently Dangerous Function	05-Nov-21	7.5	The affected application uses specific functions that could be abused through a crafted project file, which could lead to code execution, system reboot, and system shutdown. **CVE ID : CVE-2021-42543**	N/A	A-AZE-DAQF-181121/26
Deserialization of Untrusted	05-Nov-21	6.8	Project files are stored memory objects in the form of binary serialized data	N/A	A-AZE-DAQF-181121/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Data			that can later be read and deserialized again to instantiate the original objects in memory. Malicious manipulation of these files may allow an attacker to corrupt memory. **CVE ID : CVE-2021-42698**		
Cleartext Transmission of Sensitive Information	05-Nov-21	4.3	The affected product is vulnerable to cookie information being transmitted as cleartext over HTTP. An attacker can capture network traffic, obtain the user's cookie and take over the account. **CVE ID : CVE-2021-42699**	N/A	A-AZE-DAQF-181121/28
Modification of Assumed-Immutable Data (MAID)	05-Nov-21	2.6	An attacker could prepare a specially crafted project file that, if opened, would attempt to connect to the cloud and trigger a man in the middle (MiTM) attack. This could allow an attacker to obtain credentials and take over the user's cloud account. **CVE ID : CVE-2021-42701**	N/A	A-AZE-DAQF-181121/29
barrier_project					
barrier					
Improper Authentication	08-Nov-21	6.5	An issue was discovered in Barrier before 2.4.0. The barriers component (aka the server-side implementation of Barrier) does not sufficiently verify the identify of connecting	N/A	A-BAR-BARR-181121/30

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			clients. Clients can thus exploit weaknesses in the provided protocol to cause denial-of-service or stage further attacks that could lead to information leaks or integrity corruption. **CVE ID : CVE-2021-42072**		
Session Fixation	08-Nov-21	5.8	An issue was discovered in Barrier before 2.4.0. An attacker can enter an active session state with the barriers component (aka the server-side implementation of Barrier) simply by supplying a client label that identifies a valid client configuration. This label is "Unnamed" by default but could instead be guessed from hostnames or other publicly available information. In the active session state, an attacker can capture input device events from the server, and also modify the clipboard content on the server. **CVE ID : CVE-2021-42073**	https://github.com/debauchee/barrier/releases/tag/v2.4.0	A-BAR-BARR-181121/31
Use After Free	08-Nov-21	5	An issue was discovered in Barrier before 2.3.4. An unauthenticated attacker can cause a segmentation fault in the barriers component (aka the server-side implementation of Barrier) by quickly opening and closing TCP connections while sending a Hello message for each TCP	N/A	A-BAR-BARR-181121/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session. **CVE ID : CVE-2021-42074**		
Uncontrolled Resource Consumption	08-Nov-21	5	An issue was discovered in Barrier before 2.3.4. The barriers component (aka the server-side implementation of Barrier) does not correctly close file descriptors for established TCP connections. An unauthenticated remote attacker can thus cause file descriptor exhaustion in the server process, leading to denial of service. **CVE ID : CVE-2021-42075**	N/A	A-BAR-BARR-181121/33
Out-of-bounds Write	08-Nov-21	5	An issue was discovered in Barrier before 2.3.4. An attacker can cause memory exhaustion in the barriers component (aka the server-side implementation of Barrier) and barrierc by sending long TCP messages. **CVE ID : CVE-2021-42076**	N/A	A-BAR-BARR-181121/34
batch_cat_project					
batch_cat					
Incorrect Authorization	08-Nov-21	4	The Batch Cat WordPress plugin through 0.3 defines 3 custom AJAX actions, which both require authentication but are available for all roles. As a result, any authenticated user (including simple subscribers) can add/set/delete arbitrary categories to posts.	N/A	A-BAT-BATC-181121/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24788		
Bluez					
bluez					
Use After Free	04-Nov-21	6.4	An issue was discovered in gatt-database.c in BlueZ 5.61. A use-after-free can occur when a client disconnects during D-Bus processing of a WriteValue call. **CVE ID : CVE-2021-43400**	https://git.kernel.org/pub/scm/bluetooth/bluez.git/commit/?id=838c0dc7641e1c991c0f3027bf94bee4606012f8	A-BLU-BLUE-181121/36
bookingholdings					
booking.com_banner_creator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	3.5	The Booking.com Banner Creator WordPress plugin through 1.4.2 does not properly sanitize inputs when creating banners, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24646**	N/A	A-BOO-BOOK-181121/37
booking.com_product_helper					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	3.5	The Booking.com Product Helper WordPress plugin through 1.0.1 does not sanitize and escape Product Code when creating Product Shortcode, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html	N/A	A-BOO-BOOK-181121/38

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			capability is disallowed **CVE ID : CVE-2021-24645**		
bookstackapp					
bookstack					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Nov-21	4	bookstack is vulnerable to Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') **CVE ID : CVE-2021-3916**	https://huntr.dev/bounties/0be32e6b-7c48-43f0-9cec-433000ad8f64, https://github.com/bookstackapp/bookstack/commit/43830a372fc51a8793199d04a34c3f4ebdfccc7b	A-BOO-BOOK-181121/39
bootstrap_table_project					
bootstrap_table					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-21	4.3	This affects all versions of package bootstrap-table. A type confusion vulnerability can lead to a bypass of input sanitization when the input provided to the escapeHTML function is an array (instead of a string) even if the escape attribute is set. **CVE ID : CVE-2021-23472**	N/A	A-BOO-BOOT-181121/40
bracketspace					
notification					
Improper Neutralizatio	01-Nov-21	2.1	The Notification WordPress plugin is vulnerable to	https://plugins.trac.wor	A-BRA-NOTI-181121/41

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/src/classes/Utils/Settings.php file which made it possible for attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 7.2.4. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled. **CVE ID : CVE-2021-39340**	dpress.org/browser/notification/tags/7.2.4/src/classes/Utils/Settings.php#L167	
Broadcom					
emulex_hba_manager					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Nov-21	6.8	Broadcom Emulex HBA Manager/One Command Manager versions before 11.4.425.0 and 12.8.542.31, if not installed in Strictly Local Management mode, have a buffer overflow vulnerability in the remote GetDumpFile command that could allow a user to attempt various attacks. In non-secure mode, the user is unauthenticated **CVE ID : CVE-2021-42772**	https://docs.broadcom.com/doc/elx_HBAManager-Lin-RN12811-101.pdf	A-BRO-EMUL-181121/42
one_command_manager					
Buffer Copy without Checking	03-Nov-21	6.8	Broadcom Emulex HBA Manager/One Command Manager versions before	https://docs.broadcom.com/doc/elx_	A-BRO-ONE_-181121/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			11.4.425.0 and 12.8.542.31, if not installed in Strictly Local Management mode, have a buffer overflow vulnerability in the remote GetDumpFile command that could allow a user to attempt various attacks. In non-secure mode, the user is unauthenticated **CVE ID : CVE-2021-42772**	HBAManager-Lin-RN12811-101.pdf	
casap_automated_enrollment_system_project					
casap_automated_enrollment_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	4.3	Multiple Cross Site Scripting (XSS) vulnerabilities exist in SourceCodester CASAP Automated Enrollment System 1.0 via the (1) user_username and (2) category parameters in save_class.php, the (3) firstname, (4) class, and (5) status parameters in student_table.php, the (6) category and (7) class_name parameters in add_class1.php, the (8) fname, (9) mname,(10) lname, (11) address, (12) class, (13) gfname, (14) gmname, (15) glname, (16) rship, (17) status, (18) transport, and (19) route parameters in add_student.php, the (20) fname, (21) mname, (22) lname, (23) address, (24) class, (25) fgname, (26) gmname, (27) glname, (28) rship, (29) status, (30)	N/A	A-CAS-CASA-181121/44

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
			transport, and (31) route parameters in save_stud.php,the (32) status, (33) fname, and (34) lname parameters in add_user.php, the (35) username, (36) firstname, and (37) status parameters in users.php, the (38) fname, (39) lname, and (40) status parameters in save_user.php, and the (41) activity_log, (42) aprjun, (43) class, (44) janmar, (45) Julsep,(46) octdec, (47) Students and (48) users parameters in table_name. **CVE ID : CVE-2021-40261**		
chameleon_css_project					
chameleon_css					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	6.5	The Chameleon CSS WordPress plugin through 1.2 does not have any CSRF and capability checks in all its AJAX calls, allowing any authenticated user, such as subscriber to call them and perform unauthorised actions. One of AJAX call, remove_css, also does not sanitise or escape the css_id POST parameter before using it in a SQL statement, leading to a SQL Injection **CVE ID : CVE-2021-24626**	N/A	A-CHA-CHAM-181121/45
Cisco					
anyconnect_secure_mobility_client					
Improper	04-Nov-21	7.2	A vulnerability in the	https://tools	A-CIS-ANYC-

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
Privilege Management			Network Access Manager (NAM) module of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to escalate privileges on an affected device. This vulnerability is due to incorrect privilege assignment to scripts executed before user logon. An attacker could exploit this vulnerability by configuring a script to be executed before logon. A successful exploit could allow the attacker to execute arbitrary code with SYSTEM privileges. **CVE ID : CVE-2021-40124**	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-nam-priv-yCsRNUGT	181121/46
application_extension_platform					
Improper Input Validation	04-Nov-21	9	A vulnerability in the web-based management interface of certain Cisco Small Business RV Series Routers could allow an authenticated, remote attacker with administrative privileges to inject arbitrary commands into the underlying operating system and execute them using root-level privileges. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to a specific	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-cmdinjection-Z5cWFdK	A-CIS-APPL-181121/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			field in the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as a user with root-level privileges. **CVE ID : CVE-2021-40120**		
collaboration_meeting_rooms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-21	4.3	A vulnerability in Cisco Webex Video Mesh could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2021-40115**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-videomesh-xss-qjm2BDQf	A-CIS-COLL-181121/48
URL Redirection to Untrusted Site ('Open Redirect')	04-Nov-21	5.8	A vulnerability in the web-based management interface of Cisco Webex Video Mesh could allow an unauthenticated, remote attacker to redirect a user	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	A-CIS-COLL-181121/49

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a malicious web page. This vulnerability is due to improper input validation of the URL parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. Attackers may use this type of vulnerability, known as an open redirect attack, as part of a phishing attack to persuade users to unknowingly visit malicious sites. **CVE ID : CVE-2021-1500**	sco-sa-vmesh-openred-AGNRmf5	
common_services_platform_collector					
Exposure of Sensitive Information to an Unauthorized Actor	04-Nov-21	4	A vulnerability in the web-based management interface of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to access sensitive data on an affected system. This vulnerability exists because the application does not sufficiently protect sensitive data when responding to a specific API request. An attacker could exploit the vulnerability by sending a crafted HTTP request to the affected application. A successful exploit could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cspc-info-disc-KM3bGVL	A-CIS-COMM-181121/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to obtain sensitive information about the users of the application, including security questions and answers. To exploit this vulnerability an attacker would need valid Administrator credentials. Cisco expects to release software updates that address this vulnerability. **CVE ID : CVE-2021-34774**		
evolved_programmable_network_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-21	3.5	A vulnerability in the web-based management interface of Cisco Prime Infrastructure (PI) and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-xss-U2JK537j	A-CIS-EVOL-181121/51

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface or access sensitive, browser-based information. **CVE ID : CVE-2021-34784**		
policy_suite					
Use of Hard-coded Credentials	04-Nov-21	10	A vulnerability in the key-based SSH authentication mechanism of Cisco Policy Suite could allow an unauthenticated, remote attacker to log in to an affected system as the root user. This vulnerability is due to the re-use of static SSH keys across installations. An attacker could exploit this vulnerability by extracting a key from a system under their control. A successful exploit could allow the attacker to log in to an affected system as the root user. **CVE ID : CVE-2021-40119**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cps-static-key-JmS92hNv	A-CIS-POLI-181121/52
prime_access_registrar					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-21	3.5	A vulnerability in the web-based management interface of Cisco Prime Access Registrar could allow an authenticated, remote attacker to perform a stored cross-site scripting attack on an affected system. This vulnerability exists because the web-based management interface does not sufficiently validate user-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cpar-strd-xss-A4DCVETG	A-CIS-PRIM-181121/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need valid administrative credentials. Cisco expects to release software updates that address this vulnerability. **CVE ID : CVE-2021-34731**		
prime_infrastructure					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-21	3.5	A vulnerability in the web-based management interface of Cisco Prime Infrastructure (PI) and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-xss-U2JK537j	A-CIS-PRIM-181121/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2021-34784**		
umbrella					
Generation of Error Message Containing Sensitive Information	04-Nov-21	4	A vulnerability in the web-based dashboard of Cisco Umbrella could allow an authenticated, remote attacker to perform an email enumeration attack against the Umbrella infrastructure. This vulnerability is due to an overly descriptive error message on the dashboard that appears when a user attempts to modify their email address when the new address already exists in the system. An attacker could exploit this vulnerability by attempting to modify the user's email address. A successful exploit could allow the attacker to enumerate email addresses of users in the system. **CVE ID : CVE-2021-40126**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-umbrella-user-enum-S7XfJwDE	A-CIS-UMBR-181121/55
unified_communications_manager					
Improper	04-Nov-21	4	A vulnerability in the web-	https://tools	A-CIS-UNIF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P), and Cisco Unity Connection could allow an authenticated, remote attacker to access sensitive data on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to access sensitive files on the affected system. **CVE ID : CVE-2021-34701**	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-path-trav-dKCvktvO	181121/56
Cross-Site Request Forgery (CSRF)	04-Nov-21	4.3	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME),	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-csrf-	A-CIS-UNIF-181121/57

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
			and Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. These actions could include modifying the device configuration and deleting (but not creating) user accounts. **CVE ID : CVE-2021-34773**	xrTkDu3H	
unified_communications_manager_im_and_presence_service					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Nov-21	4	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-path-trav-dKCvktvO	A-CIS-UNIF-181121/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IM &amp; Presence Service (Unified CM IM&amp;P), and Cisco Unity Connection could allow an authenticated, remote attacker to access sensitive data on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to access sensitive files on the affected system. **CVE ID : CVE-2021-34701**		
Cross-Site Request Forgery (CSRF)	04-Nov-21	4.3	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-csrf-xrTkDu3H	A-CIS-UNIF-181121/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. These actions could include modifying the device configuration and deleting (but not creating) user accounts. **CVE ID : CVE-2021-34773**		
unity_connection					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Nov-21	4	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P), and Cisco Unity Connection could allow an authenticated, remote attacker to access sensitive data on an affected device. This vulnerability exists because the web-based	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-path-trav-dKCvktvO	A-CIS-UNIT-181121/60

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to access sensitive files on the affected system. **CVE ID : CVE-2021-34701**		
webex_meetings					
Improper Input Validation	04-Nov-21	5	A vulnerability in the account activation feature of Cisco Webex Meetings could allow an unauthenticated, remote attacker to send an account activation email with an activation link that points to an arbitrary domain. This vulnerability is due to insufficient validation of user-supplied parameters. An attacker could exploit this vulnerability by sending a crafted HTTP request to the account activation page of Cisco Webex Meetings. A successful exploit could allow the attacker to send to any recipient an account activation email that contains a tampered activation link, which could direct the user to an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-activation-3sdNFxcy	A-CIS-WEBE-181121/61

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker-controlled website. **CVE ID : CVE-2021-40128**		
webex_video_mesh					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-21	4.3	A vulnerability in Cisco Webex Video Mesh could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2021-40115**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-videomesh-xss-qjm2BDQf	A-CIS-WEBE-181121/62
URL Redirection to Untrusted Site ('Open Redirect')	04-Nov-21	5.8	A vulnerability in the web-based management interface of Cisco Webex Video Mesh could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the URL parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmesh-openred-AGNRmf5	A-CIS-WEBE-181121/63

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			A successful exploit could allow the attacker to redirect a user to a malicious website. Attackers may use this type of vulnerability, known as an open redirect attack, as part of a phishing attack to persuade users to unknowingly visit malicious sites. **CVE ID : CVE-2021-1500**		
Cloudera					
cloudera_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	4.3	Cloudera Manager 5.x, 6.x, 7.1.x, 7.2.x, and 7.3.x allows XSS. **CVE ID : CVE-2021-29243**	https://docs.cloudera.com/documentation/other/security-bulletins/topics/Security-Bulletin.html , https://my.cloudera.com/knowledge/TSB-2021-488-Cloudera-Manager-is-vulnerable-to-Cross-Site?id=322833	A-CLO-CLOU-181121/64
Improper Privilege Management	08-Nov-21	7.5	Cloudera Manager 7.2.4 has Incorrect Access Control, allowing Escalation of Privileges.	https://docs.cloudera.com/documentation/other	A-CLO-CLOU-181121/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30132	/security-bulletins/topics/Security-Bulletin.html, https://my.cloudera.com/knowledge/TSB-2021-491-Authorization-Bypass-in-Cloudera-Manager?id=314482	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	4.3	Cloudera Manager 5.x, 6.x, 7.1.x, 7.2.x, and 7.3.x allows XSS via the path parameter. **CVE ID : CVE-2021-32482**	https://my.cloudera.com/knowledge/TSB-2021-488-Cloudera-Manager-is-vulnerable-to-Cross-Site?id=322833, https://docs.cloudera.com/documentation/other/security-bulletins/topics/Security-Bulletin.html#cloudera_manager	A-CLO-CLOU-181121/66
Improper Privilege	08-Nov-21	5	Cloudera Manager 7.2.4 has Incorrect Access Control,	https://my.cloudera.com	A-CLO-CLOU-181121/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			allowing Escalation of Privileges to view the restricted Dashboard. **CVE ID : CVE-2021-32483**	/knowledge/TSB-2021-491-Authorization-Bypass-in-Cloudera-Manager?id=314482, https://docs.cloudera.com/documentation/other/security-bulletins/topics/Security-Bulletin.html#cloudera_manager	
hue					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	4.3	Cloudera Hue 4.6.0 allows XSS. **CVE ID : CVE-2021-29994**	https://docs.cloudera.com/documentation/other/security-bulletins/topics/Security-Bulletin.html, https://my.cloudera.com/knowledge/TSB-2021-487-Cloudera-Hue-is-vulnerable-to-Cross-Site?id=324	A-CLO-HUE-181121/68

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
				634	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	4.3	Cloudera Hue 4.6.0 allows XSS via the type parameter. **CVE ID : CVE-2021-32481**	https://docs.cloudera.com/documentation/other/security-bulletins/topics/Security-Bulletin.html#hue, https://my.cloudera.com/knowledge/TSB-2021-487-Cloudera-Hue-is-vulnerable-to-Cross-Site?id=324634	A-CLO-HUE-181121/69
codesupply					
squaretype					
Authorization Bypass Through User-Controlled Key	08-Nov-21	5	The Squaretype WordPress theme before 3.0.4 allows unauthenticated users to manipulate the query_vars used to retrieve the posts to display in one of its REST endpoint, without any validation. As a result, private and scheduled posts could be retrieved via a crafted request. **CVE ID : CVE-2021-24840**	N/A	A-COD-SQUA-181121/70
connections-pro					
connections_business_directory					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	3.5	The Connections Business Directory WordPress plugin before 10.4.3 does not escape the Address settings when creating an Entry, which could allow high privilege users to perform Cross-Site Scripting when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24794**	N/A	A-CON-CONN-181121/71
couchbase					
couchbase_server					
Cleartext Storage of Sensitive Information	02-Nov-21	5	metakv in Couchbase Server 7.0.0 uses Cleartext for Storage of Sensitive Information. Remote Cluster XDCR credentials can get leaked in debug logs. Config key tombstone purging was added in Couchbase Server 7.0.0. This issue happens when a config key, which is being logged, has a tombstone purger time-stamp attached to it. **CVE ID : CVE-2021-37842**	https://www.couchbase.com/alerts, https://docs.couchbase.com/server/current/release-notes/relnotes.html	A-COU-COUC-181121/72
Cleartext Storage of Sensitive Information	02-Nov-21	5	Couchbase Server before 6.6.3 and 7.x before 7.0.2 stores Sensitive Information in Cleartext. The issue occurs when the cluster manager forwards a HTTP request from the pluggable UI (query workbench etc) to the specific service. In the backtrace, the Basic Auth Header included in the	https://www.couchbase.com/alerts, https://docs.couchbase.com/server/current/release-notes/relnotes.html	A-COU-COUC-181121/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP request, has the "@" user credentials of the node processing the UI request. **CVE ID : CVE-2021-42763**		
Cryptopp					
crypto\\+\\+					
Observable Discrepancy	04-Nov-21	5	Crypto++ (aka Cryptopp) 8.6.0 and earlier contains a timing leakage in MakePublicKey(). There is a clear correlation between execution time and private key length, which may cause disclosure of the length information of the private key. This might allow attackers to conduct timing attacks. **CVE ID : CVE-2021-43398**	https://cryptopp.com	A-CRY-CRYP-181121/74
customer_relationship_management_system_project					
customer_relationship_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Nov-21	10	An SQL Injection vulnerability exists in Sourcecodester Customer Relationship Management System (CRM) 1.0 via the username parameter in customer/login.php. **CVE ID : CVE-2021-43130**	N/A	A-CUS-CUST-181121/75
datalust					
seq.app.emailplus					
N/A	02-Nov-21	5	Datalust Seq.App.EmailPlus (aka seq-app-htmlemail) 3.1.0-dev-00148, 3.1.0-dev-00170, and 3.1.0-dev-00176 can use cleartext SMTP on	https://github.com/datalust/seq-app-htmlemail/p	A-DAT-SEQ.-181121/76

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
			port 25 in some cases where encryption on port 465 was intended. **CVE ID : CVE-2021-43270**	ull/93	
dazzlersoftware					
coming_soon\\,_under_construction_\\&_maintenance_mode_by_dazzler					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	2.1	The Coming Soon, Under Construction & Maintenance Mode By Dazzler WordPress plugin before 1.6.7 does not sanitise or escape its description setting when outputting it in the frontend when the Coming Soon mode is enabled, even when the unfiltered_html capability is disallowed, leading to an authenticated Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24539**	N/A	A-DAZ-COMI-181121/77
deltaww					
dialink					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-21	3.5	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter supplier of the API maintenance, which may allow an attacker to remotely execute code. **CVE ID : CVE-2021-38403**	N/A	A-DEL-DIAL-181121/78
Improper Neutralizatio	03-Nov-21	3.5	Delta Electronics DIALink versions 1.2.4.0 and prior is	N/A	A-DEL-DIAL-181121/79

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter name of the API devices, which may allow an attacker to remotely execute code. **CVE ID : CVE-2021-38407**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-21	3.5	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter deviceName of the API modbusWriter-Reader, which may allow an attacker to remotely execute code. **CVE ID : CVE-2021-38411**	N/A	A-DEL-DIAL-181121/80
Uncontrolled Search Path Element	03-Nov-21	4.4	Delta Electronics DIALink versions 1.2.4.0 and prior insecurely loads libraries, which may allow an attacker to use DLL hijacking and takeover the system where the software is installed. **CVE ID : CVE-2021-38416**	N/A	A-DEL-DIAL-181121/81
Cleartext Transmission of Sensitive Information	03-Nov-21	4.3	Delta Electronics DIALink versions 1.2.4.0 and prior runs by default on HTTP, which may allow an attacker to be positioned between the traffic and perform a machine-in-the-	N/A	A-DEL-DIAL-181121/82

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			middle attack to access information without authorization. **CVE ID : CVE-2021-38418**		
Incorrect Default Permissions	03-Nov-21	4.6	Delta Electronics DIALink versions 1.2.4.0 and prior default permissions give extensive permissions to low-privileged user accounts, which may allow an attacker to modify the installation directory and upload malicious files. **CVE ID : CVE-2021-38420**	N/A	A-DEL-DIAL-181121/83
Cleartext Storage of Sensitive Information	03-Nov-21	4.6	Delta Electronics DIALink versions 1.2.4.0 and prior stores sensitive information in cleartext, which may allow an attacker to have extensive access to the application directory and escalate privileges. **CVE ID : CVE-2021-38422**	N/A	A-DEL-DIAL-181121/84
Improper Neutralization of Formula Elements in a CSV File	03-Nov-21	6.8	The tag interface of Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to an attacker injecting formulas into the tag data. Those formulas may then be executed when it is opened with a spreadsheet application. **CVE ID : CVE-2021-38424**	N/A	A-DEL-DIAL-181121/85
Improper Neutralization of Input During Web Page Generation	03-Nov-21	3.5	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript	N/A	A-DEL-DIAL-181121/86

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			code into the parameter name of the API schedule, which may allow an attacker to remotely execute code. **CVE ID : CVE-2021-38428**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-21	3.5	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter comment of the API events, which may allow an attacker to remotely execute code. **CVE ID : CVE-2021-38488**	N/A	A-DEL-DIAL-181121/87
dhis2					
dhis_2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-21	6.5	DHIS 2 is an information system for data capture, management, validation, analytics and visualization. A SQL injection security vulnerability has been found in specific versions of DHIS2. This vulnerability affects the API endpoints for /api/trackedEntityInstances and api/events in DHIS2. The system is vulnerable to attack only from users that are logged in to DHIS2, and there is no known way of exploiting the vulnerability without first being logged in as a DHIS2 user. A	https://github.com/dhis2/dhis2-core/security/advisories/GHSA-fvm5-gp3j-c7c6	A-DHI-DHIS-181121/88

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
			successful exploit of this vulnerability could allow the malicious user to read, edit and delete data in the DHIS2 instance. There are no known exploits of the security vulnerabilities addressed by these patch releases. However, we strongly recommend that all DHIS2 implementations using versions 2.32, 2.33, 2.34, 2.35 and 2.36 install these patches as soon as possible. There is no straightforward known workaround for DHIS2 instances using the Tracker functionality other than upgrading the affected DHIS2 server to one of the patches in which this vulnerability has been fixed. For implementations which do NOT use Tracker functionality, it may be possible to block all network access to POST to the /api/trackedEntityInstance and /api/events endpoints as a temporary workaround while waiting to upgrade. **CVE ID : CVE-2021-41187**		
Dolibarr					
dolibarr					
Improper Neutralization of Input During Web	10-Nov-21	4.3	Dolibarr ERP and CRM 13.0.2 allows XSS via object details, as demonstrated by > and < characters in the	N/A	A-DOL-DOLI-181121/89

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			onpointermove attribute of a BODY element to the user-management feature. **CVE ID : CVE-2021-33618**		
Improper Control of Generation of Code ('Code Injection')	10-Nov-21	7.5	The website builder module in Dolibarr 13.0.2 allows remote PHP code execution because of an incomplete protection mechanism in which system, exec, and shell_exec are blocked but backticks are not blocked. **CVE ID : CVE-2021-33816**	N/A	A-DOL-DOLI-181121/90
dotty_project					
dotty					
Access of Resource Using Incompatible Type ('Type Confusion')	03-Nov-21	7.5	This affects the package dotty before 0.1.2. A type confusion vulnerability can lead to a bypass of CVE-2021-25912 when the user-provided keys used in the path parameter are arrays. **CVE ID : CVE-2021-23624**	https://github.com/deoxxa/dotty/commit/88f61860dcc274a07a263c32cbe9d44c24ef02d7, https://snyk.io/vuln/SNYK-JS-DOTTY-1577292	A-DOT-DOTT-181121/91
doyocms_project					
doyocms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	01-Nov-21	7.5	SQL Injection vulnerability in pay.php in millken doyocms 2.3, allows attackers to execute arbitrary code, via the attribute parameter. **CVE ID : CVE-2021-26739**	N/A	A-DOY-DOYO-181121/92

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')					
Unrestricted Upload of File with Dangerous Type	01-Nov-21	7.5	Arbitrary file upload vulnerability sysupload.php in millken doyocms 2.3 allows attackers to execute arbitrary code. **CVE ID : CVE-2021-26740**	N/A	A-DOY-DOYO-181121/93
draftpress					
header_footer_code_manager					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	6.5	The Header Footer Code Manager WordPress plugin before 1.1.14 does not validate and escape the "orderby" and "order" request parameters before using them in a SQL statement when viewing the Snippets admin dashboard, leading to SQL injections **CVE ID : CVE-2021-24791**	N/A	A-DRA-HEAD-181121/94
e-dynamics					
events_made_easy					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	3.5	The Events Made Easy WordPress plugin before 2.2.24 does not sanitise and escape Custom Field Names, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24813**	https://plugins.trac.wordpress.org/changeset/2607749/	A-E-D-EVEN-181121/95
Eclipse					
paho_mqtt_c\\/c\\+\\+_client					
Out-of-bounds	03-Nov-21	7.5	In versions prior to 1.1 of the Eclipse Paho MQTT C Client, the client does not	https://github.com/eclipse/paho.m	A-ECL-PAHO-181121/96

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
Write			check rem_len size in readpacket. **CVE ID : CVE-2021-41036**	qtt.embedded-c/issues/96	
theia					
N/A	10-Nov-21	4.3	In versions of the @theia/plugin-ext component of Eclipse Theia prior to 1.18.0, Webview contents can be hijacked via postMessage(). **CVE ID : CVE-2021-41038**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=575924, https://github.com/eclipse-theia/theia/pull/10125	A-ECL-THEI-181121/97
engineers_online_portal_project					
engineers_online_portal					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-21	3.5	A Stored Cross Site Scripting (XSS) Vulneraibiilty exists in Sourcecodester Engineers Online Portal in PHP via the (1) Quiz title and (2) quiz description parameters to add_quiz.php. An attacker can leverage this vulnerability in order to run javascript commands on the web server surfers behalf, which can lead to cookie stealing and more. **CVE ID : CVE-2021-42664**	N/A	A-ENG-ENGI-181121/98
Improper Neutralization of Special Elements used in an SQL Command	05-Nov-21	7.5	An SQL Injection vulnerability exists in Sourcecodester Engineers Online Portal in PHP via the login form inside of index.php, which can allow an attacker to bypass	N/A	A-ENG-ENGI-181121/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			authentication. **CVE ID : CVE-2021-42665**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Nov-21	6.5	A SQL Injection vulnerability exists in Sourcecodester Engineers Online Portal in PHP via the id parameter to quiz_question.php, which could let a malicious user extract sensitive data from the web server and in some cases use this vulnerability in order to get a remote code execution on the remote web server. **CVE ID : CVE-2021-42666**	N/A	A-ENG-ENGI-181121/100
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Nov-21	7.5	A SQL Injection vulnerability exists in Sourcecodester Engineers Online Portal in PHP via the id parameter in the my_classmates.php web page.. As a result, an attacker can extract sensitive data from the web server and in some cases can use this vulnerability in order to get a remote code execution on the remote web server. **CVE ID : CVE-2021-42668**	N/A	A-ENG-ENGI-181121/101
Unrestricted Upload of File with Dangerous Type	05-Nov-21	10	A file upload vulnerability exists in Sourcecodester Engineers Online Portal in PHP via dashboard_teacher.php, which allows changing the avatar through teacher_avatar.php. Once an	N/A	A-ENG-ENGI-181121/102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			avatar gets uploaded it is getting uploaded to the /admin/uploads/ directory, and is accessible by all users. By uploading a php webshell containing "<?php system($_GET["cmd"]); ?>" the attacker can execute commands on the web server with - /admin/uploads/php-webshell?cmd=id. **CVE ID : CVE-2021-42669**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Nov-21	7.5	A SQL injection vulnerability exists in Sourcecodester Engineers Online Portal in PHP via the id parameter to the announcements_student.php web page. As a result a malicious user can extract sensitive data from the web server and in some cases use this vulnerability in order to get a remote code execution on the remote web server. **CVE ID : CVE-2021-42670**	N/A	A-ENG-ENGI-181121/103
Incorrect Authorization	05-Nov-21	5	An incorrect access control vulnerability exists in Sourcecodester Engineers Online Portal in PHP in nia_munoz_monitoring_system/admin/uploads. An attacker can leverage this vulnerability in order to bypass access controls and access all the files uploaded to the web server without the need of authentication	N/A	A-ENG-ENGI-181121/104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or authorization. **CVE ID : CVE-2021-42671**		
enrocrypt_project					
enrocrypt					
Use of a Broken or Risky Cryptographic Algorithm	08-Nov-21	5	EnroCrypt is a Python module for encryption and hashing. Prior to version 1.1.4, EnroCrypt used the MD5 hashing algorithm in the hashing file. Beginners who are unfamiliar with hashes can face problems as MD5 is considered an insecure hashing algorithm. The vulnerability is patched in v1.1.4 of the product. As a workaround, users can remove the `MD5` hashing function from the file `hashing.py`. **CVE ID : CVE-2021-39182**	https://github.com/Morgan-Phoenix/EnroCrypt/security/advisories/GHSA-35m5-8cvj-8783	A-ENR-ENRO-181121/105
Ericsson					
network_location					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Nov-21	6.5	In Ericsson Network Location before 2021-07-31, it is possible for an authenticated attacker to inject commands via file_name in the export functionality. **CVE ID : CVE-2021-43339**	N/A	A-ERI-NETW-181121/106
network_location_mps_gmpc21					
Improper Neutralization of Special Elements used in an	03-Nov-21	6.5	In Ericsson Network Location MPS GMPC21, it is possible to creates a new admin user with a SQL Query for file_name in the	N/A	A-ERI-NETW-181121/107

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
SQL Command ('SQL Injection')			export functionality. **CVE ID : CVE-2021-43338**		
Eset					
cyber_security					
N/A	08-Nov-21	2.1	ESET was made aware of a vulnerability in its consumer and business products for macOS that enables a user logged on to the system to stop the ESET daemon, effectively disabling the protection of the ESET security product until a system reboot. **CVE ID : CVE-2021-37850**	https://support.eset.com/en/ca8151	A-ESE-CYBE-181121/108
endpoint_antivirus					
N/A	08-Nov-21	2.1	ESET was made aware of a vulnerability in its consumer and business products for macOS that enables a user logged on to the system to stop the ESET daemon, effectively disabling the protection of the ESET security product until a system reboot. **CVE ID : CVE-2021-37850**	https://support.eset.com/en/ca8151	A-ESE-ENDP-181121/109
endpoint_security					
N/A	08-Nov-21	2.1	ESET was made aware of a vulnerability in its consumer and business products for macOS that enables a user logged on to the system to stop the ESET daemon, effectively disabling the protection of	https://support.eset.com/en/ca8151	A-ESE-ENDP-181121/110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the ESET security product until a system reboot. **CVE ID : CVE-2021-37850**		
etruel					
wpematico_rss_feed_fetcher					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	3.5	The WPeMatico RSS Feed Fetcher WordPress plugin before 2.6.12 does not escape the Feed URL added to a campaign before outputting it in an attribute, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24793**	N/A	A-ETR-WPEM-181121/111
feataholic					
maz_loader					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	6.5	The MAZ Loader â€“ Preloader Builder for WordPress plugin before 1.3.3 does not validate or escape the loader_id parameter of the mzldr shortcode, which allows users with a role as low as Contributor to perform SQL injection. **CVE ID : CVE-2021-24669**	N/A	A-FEA-MAZ_-181121/112
fimer					
aurora_vision					
Improper Restriction of Excessive Authentication Attempts	03-Nov-21	5	An issue was discovered in Fimer Aurora Vision before 2.97.10. The response to a failed login attempt discloses whether the	https://fimeronline.sharepoint.com/:b:/s/GLB-publicsp/Ee	A-FIM-AURO-181121/113

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
			username or password is wrong, helping an attacker to enumerate usernames. This can make a brute-force attack easier. **CVE ID : CVE-2021-33209**	KCnV76jG5Pn9Ud30fTlesBlk-SZS3uFU80Gt8IEWiE4Q?e=Tdmabs	
Improper Authentication	03-Nov-21	4.3	An issue was discovered in Fimer Aurora Vision before 2.97.10. An attacker can (in the WebUI) obtain plant information without authentication by reading the response of APIs from a kiosk view of a plant. **CVE ID : CVE-2021-33210**	https://fimeronline.sharepoint.com/:b:/s/GLB-publicsp/EZGyNsndR-hNgtWtDsxoRAoBchaLX4o7RWdTiX1qgD19WQ?e=I9uW0p	A-FIM-AURO-181121/114
flat_preloader_project					
flat_preloader					
Cross-Site Request Forgery (CSRF)	01-Nov-21	5	The Flat Preloader WordPress plugin before 1.5.4 does not enforce nonce checks when saving its settings, as well as does not sanitise and escape them, which could allow attackers to a make logged in admin change them with a Cross-Site Scripting payload (triggered either in the frontend or backend depending on the payload) **CVE ID : CVE-2021-24685**	N/A	A-FLA-FLAT-181121/115
Improper Neutralization of Input During Web Page Generation	01-Nov-21	3.5	The Flat Preloader WordPress plugin before 1.5.5 does not escape some of its settings when outputting them in attribute in the frontend, which could	N/A	A-FLA-FLAT-181121/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed **CVE ID : CVE-2021-24789**		
Fortinet					
forticlient					
Incorrect Authorization	02-Nov-21	7.2	An improper authorization vulnerability [CWE-285] in FortiClient for Windows versions 7.0.1 and below and 6.4.2 and below may allow a local unprivileged attacker to escalate their privileges to SYSTEM via the named pipe responsible for Forticlient updates. **CVE ID : CVE-2021-36183**	https://fortiguard.com/advisory/FG-IR-20-079	A-FOR-FORT-181121/117
Improper Control of Generation of Code ('Code Injection')	02-Nov-21	3.5	An improper control of generation of code vulnerability [CWE-94] in FortiClientMacOS versions 7.0.0 and below and 6.4.5 and below may allow an authenticated attacker to hijack the MacOS camera without the user permission via the malicious dylib file. **CVE ID : CVE-2021-42754**	https://fortiguard.com/advisory/FG-IR-21-079	A-FOR-FORT-181121/118
fortimanager					
Exposure of Resource to Wrong Sphere	03-Nov-21	2.1	An exposure of sensitive information to an unauthorized actor [CWE-200] vulnerability in FortiManager 7.0.1 and below, 6.4.6 and below, 6.2.x, 6.0.x, 5.6.0 may allow	https://fortiguard.com/advisory/FG-IR-21-103	A-FOR-FORT-181121/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a FortiGate user to see scripts from other ADOMS. **CVE ID : CVE-2021-36192**		
Incorrect Authorization	02-Nov-21	4	An improper access control vulnerability [CWE-284] in FortiManager versions 6.4.4 and 6.4.5 may allow an authenticated attacker with a restricted user profile to modify the VPN tunnel status of other VDOMs using VPN Manager. **CVE ID : CVE-2021-26107**	https://fortiguard.com/advisory/FG-IR-21-043, https://www.fortiguard.com/psirt?date=11-2021&risk=3	A-FOR-FORT-181121/120
fortiportal					
Improper Restriction of XML External Entity Reference	02-Nov-21	6.4	An improper restriction of XML external entity reference vulnerability in the parser of XML responses of FortiPortal before 6.0.6 may allow an attacker who controls the producer of XML reports consumed by FortiPortal to trigger a denial of service or read arbitrary files from the underlying file system by means of specifically crafted XML documents. **CVE ID : CVE-2021-36172**	https://fortiguard.com/advisory/FG-IR-21-104	A-FOR-FORT-181121/121
Allocation of Resources Without Limits or Throttling	02-Nov-21	5	A memory allocation with excessive size value vulnerability in the license verification function of FortiPortal before 6.0.6 may allow an attacker to perform a denial of service attack via specially crafted license blobs.	https://fortiguard.com/advisory/FG-IR-21-109	A-FOR-FORT-181121/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36174		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-21	4.3	Multiple uncontrolled resource consumption vulnerabilities in the web interface of FortiPortal before 6.0.6 may allow a single low-privileged user to induce a denial of service via multiple HTTP requests. **CVE ID : CVE-2021-36176**	https://fortiguard.com/advisory/FG-IR-21-100	A-FOR-FORT-181121/123
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Nov-21	3.5	A concurrent execution using shared resource with improper Synchronization vulnerability ('Race Condition') in the customer database interface of FortiPortal before 6.0.6 may allow an authenticated, low-privilege user to bring the underlying database data into an inconsistent state via specific coordination of web requests. **CVE ID : CVE-2021-36181**	https://fortiguard.com/advisory/FG-IR-21-102	A-FOR-FORT-181121/124
Uncontrolled Resource Consumption	02-Nov-21	4	Multiple uncontrolled resource consumption vulnerabilities in the web interface of FortiPortal before 6.0.6 may allow a single low-privileged user to induce a denial of service via multiple HTTP requests. **CVE ID : CVE-2021-32595**	https://fortiguard.com/advisory/FG-IR-21-096	A-FOR-FORT-181121/125
fortisiem					
Improper Privilege Management	02-Nov-21	4.6	A improper privilege management in Fortinet FortiSIEM Windows Agent version 4.1.4 and below	https://fortiguard.com/advisory/FG-IR-21-176	A-FOR-FORT-181121/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows attacker to execute privileged code or commands via powershell scripts **CVE ID : CVE-2021-41022**		
Cleartext Storage of Sensitive Information	02-Nov-21	2.1	A unprotected storage of credentials in Fortinet FortiSIEM Windows Agent version 4.1.4 and below allows an authenticated user to disclosure agent password due to plaintext credential storage in log files **CVE ID : CVE-2021-41023**	https://fortiguard.com/advisory/FG-IR-21-175	A-FOR-FORT-181121/127
fortiweb					
Out-of-bounds Write	02-Nov-21	7.5	A stack-based buffer overflow in Fortinet FortiWeb version 6.4.0, version 6.3.15 and below, 6.2.5 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests **CVE ID : CVE-2021-36186**	https://fortiguard.com/advisory/FG-IR-21-119	A-FOR-FORT-181121/128
Uncontrolled Resource Consumption	02-Nov-21	5	A uncontrolled resource consumption in Fortinet FortiWeb version 6.4.0, version 6.3.15 and below, 6.2.5 and below allows attacker to cause a denial of service for webserver daemon via crafted HTTP requests **CVE ID : CVE-2021-36187**	https://fortiguard.com/advisory/FG-IR-21-039	A-FOR-FORT-181121/129
fortiwlm					
Improper	02-Nov-21	4	A improper neutralization	https://forti	A-FOR-FORT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			of Special Elements used in an SQL Command ('SQL Injection') in Fortinet FortiWLM version 8.6.1 and below allows attacker to disclosure device, users and database information via crafted HTTP requests. **CVE ID : CVE-2021-36184**	guard.com/advisory/FG-IR-21-107	181121/130
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-21	6.5	A improper neutralization of special elements used in an OS command ('OS Command Injection') in Fortinet FortiWLM version 8.6.1 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests. **CVE ID : CVE-2021-36185**	https://fortiguard.com/advisory/FG-IR-21-110	A-FOR-FORT-181121/131
fullworks					
redirect_404_error_page_to_homepage_or_custom_page_with_logs					
Cross-Site Request Forgery (CSRF)	08-Nov-21	4.3	The Redirect 404 Error Page to Homepage or Custom Page with Logs WordPress plugin before 1.7.9 does not check for CSRF when deleting logs, which could allow attacker to make a logged in admin delete them via a CSRF attack **CVE ID : CVE-2021-24767**	N/A	A-FUL-REDI-181121/132
fusionpbx					
fusionpbx					
Improper Input Validation	05-Nov-21	6.5	An issue was discovered in FusionPBX before 4.5.30. The FAX file name may have	https://github.com/fusionpbx/fusio	A-FUS-FUSI-181121/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			risky characters. **CVE ID : CVE-2021-43404**	npbx/commit/487afc371e5c0dfbbc07cd002333c5bcd949d0f4	
Improper Input Validation	05-Nov-21	6.5	An issue was discovered in FusionPBX before 4.5.30. The fax_extension may have risky characters (it is not constrained to be numeric). **CVE ID : CVE-2021-43405**	https://github.com/fusionpbx/fusionpbx/commit/2d2869c1a1e874c46a8c3c5475614ce769bbbd59	A-FUS-FUSI-181121/134
Improper Input Validation	05-Nov-21	6.5	An issue was discovered in FusionPBX before 4.5.30. The fax_post_size may have risky characters (it is not constrained to preset values). **CVE ID : CVE-2021-43406**	https://github.com/fusionpbx/fusionpbx/commit/0377b2152c0e59c8f35297f9a9b6ee335a62d963	A-FUS-FUSI-181121/135
Genetechsolutions					
pie_register					
Improper Authentication	08-Nov-21	6.8	The Registration Forms â€“ User profile, Content Restriction, Spam Protection, Payment Gateways, Invitation Codes WordPress plugin before 3.1.7.6 has a flaw in the social login implementation, allowing unauthenticated attacker to login as any user on the site by only knowing their user ID or username **CVE ID : CVE-2021-24647**	N/A	A-GEN-PIE_-181121/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	7.5	The Registration Forms â€“ User profile, Content Restriction, Spam Protection, Payment Gateways, Invitation Codes WordPress plugin before 3.7.1.6 does not properly escape user data before using it in a SQL statement in the wp-json/pie/v1/login REST API endpoint, leading to an SQL injection. **CVE ID : CVE-2021-24731**	N/A	A-GEN-PIE_-181121/137
genie_wp_favicon_project					
genie_wp_favicon					
Cross-Site Request Forgery (CSRF)	08-Nov-21	4.3	The Genie WP Favicon WordPress plugin through 0.5.2 does not have CSRF in place when updating the favicon, which could allow attackers to make a logged in admin change it via a CSRF attack **CVE ID : CVE-2021-24674**	N/A	A-GEN-GENI-181121/138
getgrav					
grav					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Nov-21	5	grav is vulnerable to Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') **CVE ID : CVE-2021-3924**	https://huntr.dev/bounties/7ca13522-d0c9-4eff-a7dd-6fd1a7f205a2, https://github.com/getgrav/grav/commit/8f9c417c04b89dc	A-GET-GRAV-181121/139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				8d2de60b95e7696821b2826ce	
Gitlab					
gitlab					
N/A	05-Nov-21	2.1	In all versions of GitLab CE/EE since version 8.0, an attacker can set the pipeline schedules to be active in a project export so when an unsuspecting owner imports that project, pipelines are active by default on that project. Under specialized conditions, this may lead to information disclosure if the project is imported from an untrusted source. **CVE ID : CVE-2021-39895**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39895.json	A-GIT-GITL-181121/140
Improper Preservation of Permissions	05-Nov-21	5	Improper access control in GitLab CE/EE version 10.5 and above allowed subgroup members with inherited access to a project from a parent group to still have access even after the subgroup is transferred **CVE ID : CVE-2021-39897**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39897.json	A-GIT-GITL-181121/141
Exposure of Resource to Wrong Sphere	05-Nov-21	5	In all versions of GitLab CE/EE since version 10.6, a project export leaks the external webhook token value which may allow access to the project which it was exported from. **CVE ID : CVE-2021-39898**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39898.json	A-GIT-GITL-181121/142
N/A	05-Nov-21	4	In all versions of GitLab	https://gitla	A-GIT-GITL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CE/EE since version 11.10, an admin of a group can see the SCIM token of that group by visiting a specific endpoint. **CVE ID : CVE-2021-39901**	b.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39901.json	181121/143
Incorrect Authorization	04-Nov-21	4	Incorrect Authorization in GitLab CE/EE 13.4 or above allows a user with guest membership in a project to modify the severity of an incident. **CVE ID : CVE-2021-39902**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39902.json	A-GIT-GITL-181121/144
Incorrect Authorization	04-Nov-21	4	In all versions of GitLab CE/EE since version 13.0, a privileged user, through an API call, can change the visibility level of a group or a project to a restricted option even after the instance administrator sets that visibility option as restricted in settings. **CVE ID : CVE-2021-39903**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39903.json	A-GIT-GITL-181121/145
Incorrect Authorization	05-Nov-21	4	An Improper Access Control vulnerability in the GraphQL API in GitLab CE/EE since version 13.1 allows a Merge Request creator to resolve discussions and apply suggestions after a project owner has locked the Merge Request **CVE ID : CVE-2021-39904**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39904.json	A-GIT-GITL-181121/146
N/A	05-Nov-21	4	An information disclosure vulnerability in the GitLab CE/EE API since version 8.9.6 allows a user to see	https://gitlab.com/gitlab-org/cves/-/blob/maste	A-GIT-GITL-181121/147

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
			basic information on private groups that a public project has been shared with **CVE ID : CVE-2021-39905**	r/2021/CVE-2021-39905.json	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-21	4.3	Improper validation of ipynb files in GitLab CE/EE version 13.5 and above allows an attacker to execute arbitrary JavaScript code on the victim's behalf. **CVE ID : CVE-2021-39906**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39906.json	A-GIT-GITL-181121/148
Allocation of Resources Without Limits or Throttling	05-Nov-21	5	A potential DOS vulnerability was discovered in GitLab CE/EE starting with version 13.7. The stripping of EXIF data from certain images resulted in high CPU usage. **CVE ID : CVE-2021-39907**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39907.json	A-GIT-GITL-181121/149
Improper Verification of Cryptographic Signature	05-Nov-21	3.5	Lack of email address ownership verification in the CODEOWNERS feature in all versions of GitLab EE since version 11.3 allows an attacker to bypass CODEOWNERS Merge Request approval requirement under rare circumstances **CVE ID : CVE-2021-39909**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39909.json	A-GIT-GITL-181121/150
Incorrect Authorization	05-Nov-21	4	An improper access control flaw in GitLab CE/EE since version 13.9 exposes private email address of Issue and Merge Requests assignee to Webhook data consumers	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39911.json	A-GIT-GITL-181121/151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39911		
Allocation of Resources Without Limits or Throttling	05-Nov-21	5	A potential DoS vulnerability was discovered in GitLab CE/EE starting with version 13.7. Using a malformed TIFF images was possible to trigger memory exhaustion. **CVE ID : CVE-2021-39912**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39912.json	A-GIT-GITL-181121/152
Improper Privilege Management	05-Nov-21	7.2	Accidental logging of system root password in the migration log in all versions of GitLab CE/EE allows an attacker with local file system access to obtain system root-level privileges **CVE ID : CVE-2021-39913**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39913.json	A-GIT-GITL-181121/153
Allocation of Resources Without Limits or Throttling	04-Nov-21	5	A regular expression denial of service issue in GitLab versions 8.13 to 14.2.5, 14.3.0 to 14.3.3 and 14.4.0 could cause excessive usage of resources when a specially crafted username was used when provisioning a new user **CVE ID : CVE-2021-39914**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39914.json	A-GIT-GITL-181121/154
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-21	3.5	A stored Cross-Site Scripting vulnerability in the DataDog integration in GitLab CE/EE version 13.7 and above allows an attacker to execute arbitrary JavaScript code on the victim's behalf **CVE ID : CVE-2021-22260**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22260.json, https://gitlab.com/gitlab-org/gitlab/-/issues/336	A-GIT-GITL-181121/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				614	
GNU					
glibc					
N/A	04-Nov-21	5	** DISPUTED ** In iconvdata/iso-2022-jp-3.c in the GNU C Library (aka glibc) 2.34, remote attackers can force iconv() to emit a spurious '\0' character via crafted ISO-2022-JP-3 data that is accompanied by an internal state reset. This may affect data integrity in certain iconv() use cases. NOTE: the vendor states "the bug cannot be invoked through user input and requires iconv to be invoked with a NULL inbuf, which ought to require a separate application bug to do so unintentionally. Hence there's no security impact to the bug." **CVE ID : CVE-2021-43396**	N/A	A-GNU-GLIB-181121/156
hurd					
Incorrect Authorization	07-Nov-21	8.5	An issue was discovered in GNU Hurd before 0.9 20210404-9. When trying to exec a setuid executable, there's a window of time when the process already has the new privileges, but still refers to the old task and is accessible through the old process port. This can be exploited to get full root access.	https://salsa.debian.org/hurd-team/hurd/-/blob/4d1b079411e2f40576e7b58f9b5b78f733a2beda/debian/patches/0034-proc-Use-UIDs-	A-GNU-HURD-181121/157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-43411	for-evaluating-permissions.patch, https://lists.gnu.org/archive/html/bug-hurd/2021-05/msg00079.html	
Use After Free	07-Nov-21	7.2	An issue was discovered in GNU Hurd before 0.9 20210404-9. libports accepts fake notification messages from any client on any port, which can lead to port use-after-free. This can be exploited for local privilege escalation to get full root access. **CVE ID : CVE-2021-43412**	https://lists.gnu.org/archive/html/bug-hurd/2021-05/msg00079.html, https://www.mail-archive.com/bug-hurd@gnu.org/msg32116.html	A-GNU-HURD-181121/158
N/A	07-Nov-21	9	An issue was discovered in GNU Hurd before 0.9 20210404-9. A single pager port is shared among everyone who mmaps a file, allowing anyone to modify any files that they can read. This can be trivially exploited to get full root access. **CVE ID : CVE-2021-43413**	https://lists.gnu.org/archive/html/bug-hurd/2021-05/msg00079.html, https://lists.gnu.org/archive/html/bug-hurd/2002-11/msg00263.html, https://ww	A-GNU-HURD-181121/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				w.mail-archive.com/bug-hurd@gnu.org/msg32113.html	
Incorrect Authorization	07-Nov-21	6.9	An issue was discovered in GNU Hurd before 0.9 20210404-9. The use of an authentication protocol in the proc server is vulnerable to man-in-the-middle attacks, which can be exploited for local privilege escalation to get full root access. **CVE ID : CVE-2021-43414**	https://www.mail-archive.com/bug-hurd@gnu.org/msg32114.html, https://lists.gnu.org/archive/html/bug-hurd/2021-05/msg00079.html	A-GNU-HURD-181121/160
Golang					
go					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Nov-21	4.3	ImportedSymbols in debug/macho (for Open or OpenFat) in Go before 1.16.10 and 1.17.x before 1.17.3 Accesses a Memory Location After the End of a Buffer, aka an out-of-bounds slice situation. **CVE ID : CVE-2021-41771**	https://groups.google.com/g/golang-announce/c/0fM21h43arc	A-GOL-GO-181121/161
Improper Input Validation	08-Nov-21	4.3	Go before 1.16.10 and 1.17.x before 1.17.3 allows an archive/zip Reader.Open panic via a crafted ZIP archive containing an invalid name or an empty filename field.	https://groups.google.com/g/golang-announce/c/0fM21h43arc	A-GOL-GO-181121/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-41772		
Google					
chrome					
Use After Free	02-Nov-21	6.8	Use after free in Garbage Collection in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37977**	https://crbug.com/1252878, https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop.html	A-GOO-CHRO-181121/163
Out-of-bounds Write	02-Nov-21	6.8	Heap buffer overflow in Blink in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37978**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop.html, https://crbug.com/1236318	A-GOO-CHRO-181121/164
Out-of-bounds Write	02-Nov-21	6.8	heap buffer overflow in WebRTC in Google Chrome prior to 94.0.4606.81 allowed a remote attacker who convinced a user to browse to a malicious website to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37979**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop.html, https://crbug.com/1247260	A-GOO-CHRO-181121/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Nov-21	4.3	Inappropriate implementation in Sandbox in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially bypass site isolation via Windows. **CVE ID : CVE-2021-37980**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop.html, https://crbug.com/1254631	A-GOO-CHRO-181121/166
Out-of-bounds Write	02-Nov-21	6.8	Heap buffer overflow in Skia in Google Chrome prior to 95.0.4638.54 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2021-37981**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html, https://crbug.com/1246631	A-GOO-CHRO-181121/167
Use After Free	02-Nov-21	6.8	Use after free in Incognito in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37982**	https://crbug.com/1248661, https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-181121/168
Use After Free	02-Nov-21	6.8	Use after free in Dev Tools in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to	https://chromereleases.googleblog.com/2021/10	A-GOO-CHRO-181121/169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37983**	/stable-channel-update-for-desktop_19.html, https://crbug.com/1249810	
Out-of-bounds Write	02-Nov-21	6.8	Heap buffer overflow in PDFium in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37984**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html, https://crbug.com/1253399	A-GOO-CHRO-181121/170
Use After Free	02-Nov-21	6.8	Use after free in V8 in Google Chrome prior to 95.0.4638.54 allowed a remote attacker who had convinced a user to allow for connection to debugger to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37985**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html, https://crbug.com/1241860	A-GOO-CHRO-181121/171
Out-of-bounds Write	02-Nov-21	6.8	Heap buffer overflow in Settings in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to engage with Dev Tools to potentially exploit heap corruption via a crafted HTML page.	https://crbug.com/1242404, https://chromereleases.googleblog.com/2021/10/stable-	A-GOO-CHRO-181121/172

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
			CVE ID : CVE-2021-37986	channel-update-for-desktop_19.html	
Use After Free	02-Nov-21	6.8	Use after free in Network APIs in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37987**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html, https://crbug.com/1206928	A-GOO-CHRO-181121/173
Use After Free	02-Nov-21	6.8	Use after free in Profiles in Google Chrome prior to 95.0.4638.54 allowed a remote attacker who convinced a user to engage in specific gestures to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37988**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html, https://crbug.com/1228248	A-GOO-CHRO-181121/174
N/A	02-Nov-21	4.3	Inappropriate implementation in Blink in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to abuse content security policy via a crafted HTML page. **CVE ID : CVE-2021-37989**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html, https://crbug.com/1233067	A-GOO-CHRO-181121/175

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
N/A	02-Nov-21	4.3	Inappropriate implementation in WebView in Google Chrome on Android prior to 95.0.4638.54 allowed a remote attacker to leak cross-origin data via a crafted app. **CVE ID : CVE-2021-37990**	https://crbug.com/1247395, https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-181121/176
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Nov-21	5.1	Race in V8 in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37991**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html, https://crbug.com/1250660	A-GOO-CHRO-181121/177
Out-of-bounds Read	02-Nov-21	6.8	Out of bounds read in WebAudio in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37992**	https://crbug.com/1253746, https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-181121/178
Use After Free	02-Nov-21	6.8	Use after free in PDF Accessibility in Google Chrome prior to 95.0.4638.54 allowed a	https://chromereleases.googleblog.com/2021/10	A-GOO-CHRO-181121/179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37993**	/stable-channel-update-for-desktop_19.html, https://crbug.com/1255332	
N/A	02-Nov-21	4.3	Inappropriate implementation in iFrame Sandbox in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2021-37994**	N/A	A-GOO-CHRO-181121/180
N/A	02-Nov-21	4.3	Inappropriate implementation in WebApp Installer in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially overlay and spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-37995**	https://crbug.com/1242315, https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-181121/181
Improper Input Validation	02-Nov-21	4.3	Insufficient validation of untrusted input Downloads in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to bypass navigation restrictions via a malicious file. **CVE ID : CVE-2021-37996**	https://crbug.com/1243020, https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.	A-GOO-CHRO-181121/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				html	
tensorflow					
Integer Overflow or Wraparound	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions the implementation of \`tf.math.segment_*\` operations results in a \`CHECK\`-fail related abort (and denial of service) if a segment id in \`segment_ids\` is large. This is similar to CVE-2021-29584 (and similar other reported vulnerabilities in TensorFlow, localized to specific APIs): the implementation (both on CPU and GPU) computes the output shape using \`AddDim\`. However, if the number of elements in the tensor overflows an \`int64_t\` value, \`AddDim\` results in a \`CHECK\` failure which provokes a \`std::abort\`. Instead, code should use \`AddDimWithStatus\`. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41195**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-cq76-mxrc-vchh, https://github.com/tensorflow/tensorflow/commit/e9c81c1e1a9cd8dd31f4e83676cab61b60658429, https://github.com/tensorflow/tensorflow/pull/51733	A-GOO-TENS-181121/183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions the Keras pooling layers can trigger a segfault if the size of the pool is 0 or if a dimension is negative. This is due to the TensorFlow's implementation of pooling operations where the values in the sliding window are not checked to be strictly positive. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41196**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-m539-j985-hcr8, https://github.com/tensorflow/tensorflow/commit/12b1ff82b3f26ff8de17e58703231d5a02ef1b8b	A-GOO-TENS-181121/184
Integer Overflow or Wraparound	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions TensorFlow allows tensor to have a large number of dimensions and each dimension can be as large as desired. However, the total number of elements in a tensor must fit within an `int64_t`. If an overflow occurs, `MultiplyWithoutOverflow` would return a negative result. In the majority of TensorFlow codebase this	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-prcg-wp5q-rv7p, https://github.com/tensorflow/tensorflow/commit/a871989d7b6c18cdebf2fb4f0e5c5b62fbc19edf	A-GOO-TENS-181121/185

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
			then results in a `CHECK`-failure. Newer constructs exist which return a `Status` instead of crashing the binary. This is similar to CVE-2021-29584. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41197**		
Integer Overflow or Wraparound	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions if `tf.tile` is called with a large input argument then the TensorFlow process will crash due to a `CHECK`-failure caused by an overflow. The number of elements in the output tensor is too much for the `int64_t` type and the overflow is detected via a `CHECK` statement. This aborts the process. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41198**	https://github.com/tensorflow/tensorflow/commit/9294094df6fea79271778eb7e7ae1bad8b5ef98f, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-2p25-55c9-h58q	A-GOO-TENS-181121/186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions if `tf.image.resize` is called with a large input argument then the TensorFlow process will crash due to a `CHECK`-failure caused by an overflow. The number of elements in the output tensor is too much for the `int64_t` type and the overflow is detected via a `CHECK` statement. This aborts the process. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41199**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-5hx2-qx8j-qjqm, https://github.com/tensorflow/tensorflow/commit/e5272d4204ff5b46136a1ef1204fc00597e21837	A-GOO-TENS-181121/187
Reachable Assertion	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions if `tf.summary.create_file_writer` is called with non-scalar arguments code crashes due to a `CHECK`-fail. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gh8h-7j2j-qv4f, https://github.com/tensorflow/tensorflow/commit/874bda09e6702cd50bac90b453	A-GOO-TENS-181121/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supported range. **CVE ID : CVE-2021-41200**	b50bcc65b2769e	
Access of Uninitialized Pointer	05-Nov-21	4.6	TensorFlow is an open source platform for machine learning. In affeced versions during execution, `EinsumHelper::ParseEquation()` is supposed to set the flags in `input_has_ellipsis` vector and `*output_has_ellipsis` boolean to indicate whether there is ellipsis in the corresponding inputs and output. However, the code only changes these flags to `true` and never assigns `false`. This results in unitialized variable access if callers assume that `EinsumHelper::ParseEquation()` always sets these flags. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41201**	https://github.com/tensorflow/tensorflow/commit/f09caa532b6e1ac8d2aa61b7832c78c5b79300c6, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-j86v-p27c-73fm	A-GOO-TENS-181121/189
Incorrect Conversion between Numeric Types	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions while calculating the size of the output within the `tf.range` kernel, there is a conditional statement of	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-xrqm-fpgr-6hhx,	A-GOO-TENS-181121/190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			type `int64 = condition ? int64 : double`. Due to C++ implicit conversion rules, both branches of the condition will be cast to `double` and the result would be truncated before the assignment. This result in overflows. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41202**	https://github.com/tensorflow/tensorflow/commit/1b0e0ec27e7895b9985076eab32445026ae5ca94	
Insufficient Verification of Data Authenticity	05-Nov-21	4.6	TensorFlow is an open source platform for machine learning. In affected versions an attacker can trigger undefined behavior, integer overflows, segfaults and `CHECK`-fail crashes if they can change saved checkpoints from outside of TensorFlow. This is because the checkpoints loading infrastructure is missing validation for invalid file formats. The fixes will be included in TensorFlow 2.7.0. We will also cherrypick these commits on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-7pxj-m4jf-r6h2, https://github.com/tensorflow/tensorflow/commit/368af875869a204b4ac552b9ddda59f6a46a56ec	A-GOO-TENS-181121/191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supported range. **CVE ID : CVE-2021-41203**		
Access of Uninitialized Pointer	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions during TensorFlow's Grappler optimizer phase, constant folding might attempt to deep copy a resource tensor. This results in a segfault, as these tensors are supposed to not change. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41204**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-786j-5qwq-r36x	A-GOO-TENS-181121/192
Out-of-bounds Read	05-Nov-21	3.6	TensorFlow is an open source platform for machine learning. In affected versions the shape inference functions for the `QuantizeAndDequantizeV*` operations can trigger a read outside of bounds of heap allocated array. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-49rx-x2rw-pc6f, https://github.com/tensorflow/tensorflow/commit/7cf73a2274732c9d82af51c2bc2cf90d13cd7e6d	A-GOO-TENS-181121/193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-41205		
Improper Validation of Integrity Check Value	05-Nov-21	4.6	TensorFlow is an open source platform for machine learning. In affected versions several TensorFlow operations are missing validation for the shapes of the tensor arguments involved in the call. Depending on the API, this can result in undefined behavior and segfault or `CHECK`-fail related crashes but in some scenarios writes and reads from heap populated arrays are also possible. We have discovered these issues internally via tooling while working on improving/testing GPU op determinism. As such, we don't have reproducers and there will be multiple fixes for these issues. These fixes will be included in TensorFlow 2.7.0. We will also cherrypick these commits on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41206**	https://github.com/tensorflow/tensorflow/commit/68422b215e618df5ad375bcdc6d2052e9fd3080a, https://github.com/tensorflow/tensorflow/commit/4d74d8a00b07441cba090a02e0dd9ed385145bf4	A-GOO-TENS-181121/194
Divide By Zero	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `ParallelConcat` misses	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-	A-GOO-TENS-181121/195

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
			some input validation and can produce a division by 0. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41207**	7v94-64hj-m82h, https://github.com/tensorflow/tensorflow/commit/f2c3931113eaafe9ef558faaddd48e00a6606235	
NULL Pointer Dereference	05-Nov-21	4.6	TensorFlow is an open source platform for machine learning. In affected versions the code for boosted trees in TensorFlow is still missing validation. As a result, attackers can trigger denial of service (via dereferencing `nullptr`s or via `CHECK`-failures) as well as abuse undefined behavior (binding references to `nullptr`s). An attacker can also read and write from heap buffers, depending on the API that gets used and the arguments that are passed to the call. Given that the boosted trees implementation in TensorFlow is unmaintained, it is recommend to no longer use these APIs. We will deprecate TensorFlow's boosted trees APIs in subsequent releases. The fix	https://github.com/tensorflow/tensorflow/commit/5c8c9a8bfe750f9743d0c859bae112060b216f5c, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-57wx-m983-2f88	A-GOO-TENS-181121/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41208**		
Divide By Zero	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions the implementations for convolution operators trigger a division by 0 if passed empty filter tensor arguments. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41209**	https://github.com/tensorflow/tensorflow/commit/f2c3931113eaafe9ef558faaddd48e00a6606235, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-6hpv-v2rx-c5g6	A-GOO-TENS-181121/197
Out-of-bounds Read	05-Nov-21	3.6	TensorFlow is an open source platform for machine learning. In affected versions the shape inference functions for `SparseCountSparseOutput` can trigger a read outside of bounds of heap allocated array. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1,	https://github.com/tensorflow/tensorflow/commit/701cfaca222a82afbeeb17496bd718baa65a67d2, https://github.com/tensorflow/tensorflow/secu	A-GOO-TENS-181121/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41210**	rity/advisories/GHSA-m342-ff57-4jcc	
Out-of-bounds Read	05-Nov-21	3.6	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `QuantizeV2` can trigger a read outside of bounds of heap allocated array. This occurs whenever `axis` is a negative value less than `-1`. In this case, we are accessing data before the start of a heap buffer. The code allows `axis` to be an optional argument (`s` would contain an `error::NOT_FOUND` error code). Otherwise, it assumes that `axis` is a valid index into the dimensions of the `input` tensor. If `axis` is less than `-1` then this results in a heap OOB read. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, as this version is the only one that is also affected. **CVE ID : CVE-2021-41211**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-cvgx-3v3q-m36c, https://github.com/tensorflow/tensorflow/commit/a0d64445116c43cf46a5666bd4eee28e7a82f244	A-GOO-TENS-181121/199
Out-of-bounds Read	05-Nov-21	3.6	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for	https://github.com/tensorflow/tensorflow/security/advisori	A-GOO-TENS-181121/200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			`tf.ragged.cross` can trigger a read outside of bounds of heap allocated array. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41212**	es/GHSA-fr77-rrx3-cp7g, https://github.com/tensorflow/tensorflow/commit/fa6b7782fbb14aa08d767bc799c531f5e1fb3bb8	
Improper Locking	05-Nov-21	4.3	TensorFlow is an open source platform for machine learning. In affected versions the code behind `tf.function` API can be made to deadlock when two `tf.function` decorated Python functions are mutually recursive. This occurs due to using a non-reentrant `Lock` Python object. Loading any model which contains mutually recursive functions is vulnerable. An attacker can cause denial of service by causing users to load such models and calling a recursive `tf.function`, although this is not a frequent scenario. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in	https://github.com/tensorflow/tensorflow/commit/afac8158d43691661ad083f6dd9e56f327c1dcb7, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h67m-xg8f-fxcf	A-GOO-TENS-181121/201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supported range. **CVE ID : CVE-2021-41213**		
Access of Uninitialized Pointer	05-Nov-21	4.6	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `tf.ragged.cross` has an undefined behavior due to binding a reference to `nullptr`. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41214**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vwhq-49r4-gj9v, https://github.com/tensorflow/tensorflow/commit/fa6b7782fbb14aa08d767bc799c531f5e1fb3bb8	A-GOO-TENS-181121/202
NULL Pointer Dereference	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `DeserializeSparse` can trigger a null pointer dereference. This is because the shape inference function assumes that the `serialize_sparse` tensor is a tensor with positive rank (and having `3` as the last dimension). The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these	https://github.com/tensorflow/tensorflow/commit/d3738dd70f1c9ceb547258cbb82d853da8771850, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-x3v8-c8qx-3j3r	A-GOO-TENS-181121/203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are also affected and still in supported range. **CVE ID : CVE-2021-41215**		
Out-of-bounds Write	05-Nov-21	4.6	TensorFlow is an open source platform for machine learning. In affected versions the shape inference function for `Transpose` is vulnerable to a heap buffer overflow. This occurs whenever `perm` contains negative elements. The shape inference function does not validate that the indices in `perm` are all valid. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41216**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-3ff2-r28g-w7h9, https://github.com/tensorflow/tensorflow/commit/c79ba87153ee343401dbe9d1954d7f79e521eb14	A-GOO-TENS-181121/204
NULL Pointer Dereference	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions the process of building the control flow graph for a TensorFlow model is vulnerable to a null pointer exception when nodes that should be paired are not. This occurs because the code assumes that the first node in the pairing (e.g., an `Enter` node) always exists when encountering the	https://github.com/tensorflow/tensorflow/commit/05cbebd3c6bb8f517a158b0155debb8df79017ff, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-	A-GOO-TENS-181121/205

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
			second node (e.g., an `Exit` node). When this is not the case, `parent` is `nullptr` so dereferencing it causes a crash. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41217**	5crj-c72x-m7gq	
Divide By Zero	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `AllToAll` can be made to execute a division by 0. This occurs whenever the `split_count` argument is 0. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41218**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9crf-c6qr-r273, https://github.com/tensorflow/tensorflow/commit/a8ad3e5e79c75f36edb81e0ba3f3c0c5442aeddc	A-GOO-TENS-181121/206
Out-of-bounds Read	05-Nov-21	4.6	TensorFlow is an open source platform for machine learning. In affected versions the code for sparse matrix multiplication is vulnerable to undefined behavior via binding a reference to	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-4f99-p9c2-3j8x,	A-GOO-TENS-181121/207

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
			`nullptr`. This occurs whenever the dimensions of `a` or `b` are 0 or less. In the case on one of these is 0, an empty output tensor should be allocated (to conserve the invariant that output tensors are always allocated when the operation is successful) but nothing should be written to it (that is, we should return early from the kernel implementation). Otherwise, attempts to write to this empty tensor would result in heap OOB access. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41219**	https://github.com/tensorflow/tensorflow/commit/e6cf28c72ba2eb949ca950d834dd6d66bb01cfae	
Use After Free	05-Nov-21	4.6	TensorFlow is an open source platform for machine learning. In affected versions the async implementation of `CollectiveReduceV2` suffers from a memory leak and a use after free. This occurs due to the asynchronous computation and the fact that objects that have been `std::move()`d from are still	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gpfh-jvf9-7wg5, https://github.com/tensorflow/tensorflow/commit/ca38dab	A-GOO-TENS-181121/208

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
			accessed. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, as this version is the only one that is also affected. **CVE ID : CVE-2021-41220**	9d3ee66c5de06f11af9a4b1200da5ef75	
Out-of-bounds Write	05-Nov-21	4.6	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for the `Cudnn*` operations in TensorFlow can be tricked into accessing invalid memory, via a heap buffer overflow. This occurs because the ranks of the `input`, `input_h` and `input_c` parameters are not validated, but code assumes they have certain values. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41221**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-cqv6-3phm-hcwx, https://github.com/tensorflow/tensorflow/commit/af5fcebb37c8b5d71c237f4e59c6477015c78ce6	A-GOO-TENS-181121/209
N/A	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `SplitV` can trigger a segfault is an attacker supplies negative arguments. This occurs	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-cpf4-wx82-gxp6,	A-GOO-TENS-181121/210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			whenever `size_splits` contains more than one value and at least one value is negative. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41222**	https://github.com/tensorflow/tensorflow/commit/25d622ffc432acc736b14ca3904177579e733cc6	
Out-of-bounds Read	05-Nov-21	3.6	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `FusedBatchNorm` kernels is vulnerable to a heap OOB access. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41223**	https://github.com/tensorflow/tensorflow/commit/aab9998916c2ffbd8f0592059fad352622f89cda, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f54p-f6jp-4rhr	A-GOO-TENS-181121/211
Out-of-bounds Read	05-Nov-21	3.6	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `SparseFillEmptyRows` can be made to trigger a heap OOB access. This occurs whenever the size of `indices` does not match the	https://github.com/tensorflow/tensorflow/commit/67bfd9feeecfb3c61d80f0e46d89c170fbee682b, https://gith	A-GOO-TENS-181121/212

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
			size of `values`. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41224**	ub.com/tensorflow/tensorflow/security/advisories/GHSA-rg3m-hqc5-344v	
Use of Uninitialized Resource	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions TensorFlow's Grappler optimizer has a use of unitialized variable. If the `train_nodes` vector (obtained from the saved model that gets optimized) does not contain a `Dequeue` node, then `dequeue_node` is left unitialized. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41225**	https://github.com/tensorflow/tensorflow/commit/68867bf01239d9e1048f98cbad185bf4761bedd3, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-7r94-xv9v-63jw	A-GOO-TENS-181121/213
Out-of-bounds Read	05-Nov-21	3.6	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `SparseBinCount` is vulnerable to a heap OOB	https://github.com/tensorflow/tensorflow/commit/f410212e373eb2aec4c9e60bf37	A-GOO-TENS-181121/214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access. This is because of missing validation between the elements of the `values` argument and the shape of the sparse output. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41226**	02eba99a38aba, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-374m-jm66-3vj8	
Out-of-bounds Read	05-Nov-21	2.1	TensorFlow is an open source platform for machine learning. In affected versions the `ImmutableConst` operation in TensorFlow can be tricked into reading arbitrary memory contents. This is because the `tstring` TensorFlow string class has a special case for memory mapped strings but the operation itself does not offer any support for this datatype. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41227**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-j8c8-67vp-6mx7, https://github.com/tensorflow/tensorflow/commit/3712a2d3455e6ccb924daa5724a3652a86f6b585	A-GOO-TENS-181121/215
Improper Control of	05-Nov-21	4.6	TensorFlow is an open source platform for	https://github.com/tens	A-GOO-TENS-181121/216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			machine learning. In affected versions TensorFlow's `saved_model_cli` tool is vulnerable to a code injection as it calls `eval` on user supplied strings. This can be used by attackers to run arbitrary code on the plaform where the CLI tool runs. However, given that the tool is always run manually, the impact of this is not severe. We have patched this by adding a `safe` flag which defaults to `True` and an explicit warning for users. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range. **CVE ID : CVE-2021-41228**	orflow/tensorflow/commit/8b202f08d52e8206af2bdb2112a62fafbc546ec7, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-3rcw-9p9x-582v	
grafana					
grafana					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-21	4.3	Grafana is an open-source platform for monitoring and observability. In affected versions if an attacker is able to convince a victim to visit a URL referencing a vulnerable page, arbitrary JavaScript content may be executed within the context of the victim's browser. The user visiting the malicious	https://github.com/grafana/grafana/commit/3cb5214fa45eb5a571fd70d6c6edf0d729983f82, https://github.com/grafana/grafana	A-GRA-GRAF-181121/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			link must be unauthenticated and the link must be for a page that contains the login button in the menu bar. The url has to be crafted to exploit AngularJS rendering and contain the interpolation binding for AngularJS expressions. AngularJS uses double curly braces for interpolation binding: {{ }} ex: {{constructor.constructor(â€˜alert(1)â€™)()}}. When the user follows the link and the page renders, the login button will contain the original link with a query parameter to force a redirect to the login page. The URL is not validated and the AngularJS rendering engine will execute the JavaScript expression contained in the URL. Users are advised to upgrade as soon as possible. If for some reason you cannot upgrade, you can use a reverse proxy or similar to block access to block the literal string {{ in the path. **CVE ID : CVE-2021-41174**	/commit/31b78d51c693d828720a5b285107a50e6024c912, https://github.com/grafana/grafana/commit/fb85ed691290d211a5baa44d9a641ab137f0de88	
graphql					
graphiql					
Improper Neutralization of Input During Web	04-Nov-21	2.6	GraphiQL is the reference implementation of this monorepo, GraphQL IDE, an official project under the	https://github.com/graphql/graphiql/security/ad	A-GRA-GRAP-181121/218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			GraphQL Foundation. All versions of graphiql older than graphiql@1.4.7 are vulnerable to compromised HTTP schema introspection responses or schema prop values with malicious GraphQL type names, exposing a dynamic XSS attack surface that can allow code injection on operation autocomplete. In order for the attack to take place, the user must load a vulnerable schema in graphiql. There are a number of ways that can occur. By default, the schema URL is not attacker-controllable in graphiql or in its suggested implementations or examples, leaving only very complex attack vectors. If a custom implementation of graphiql's fetcher allows the schema URL to be set dynamically, such as a URL query parameter like ?endpoint= in graphql-playground, or a database provided value, then this custom graphiql implementation is vulnerable to phishing attacks, and thus much more readily available, low or no privelege level xss attacks. The URLs could look like any generic looking graphql schema	visories/GHSA-x4r7-m2q9-69c8, https://github.com/graphql/graphiql/commit/cb237eeeaf7333c4954c752122261db7520f7bf4	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			URL. It should be noted that desktop clients such as Altair, Insomnia, Postwoman, do not appear to be impacted by this. This vulnerability does not impact codemirror-graphql, monaco-graphql or other dependents, as it exists in onHasCompletion.ts in graphiql. It does impact all forks of graphiql, and every released version of graphiql. **CVE ID : CVE-2021-41248**		
playground					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-21	2.6	GraphQL Playground is a GraphQL IDE for development of graphQL focused applications. All versions of graphql-playground-react older than graphql-playground-react@1.7.28 are vulnerable to compromised HTTP schema introspection responses or schema prop values with malicious GraphQL type names, exposing a dynamic XSS attack surface that can allow code injection on operation autocomplete. In order for the attack to take place, the user must load a malicious schema in graphql-playground. There are several ways this can occur, including by specifying the URL to a	https://github.com/graphql/graphql-playground/security/advisories/GHSA-59r9-6jp6-jcm7, https://github.com/graphql/graphql-playground/commit/b8a956006835992f12c46b90384a79ab82bcadad	A-GRA-PLAY-181121/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious schema in the endpoint query parameter. If a user clicks on a link to a GraphQL Playground installation that specifies a malicious server, arbitrary JavaScript can run in the user's browser, which can be used to exfiltrate user credentials or other harmful goals. If you are using graphql-playground-react directly in your client app, upgrade to version 1.7.28 or later. **CVE ID : CVE-2021-41249**		
gtranslate					
google_language_translator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	3.5	The Translate WordPress â€“ Google Language Translator WordPress plugin before 6.0.12 does not sanitise and escape some of its settings before outputting it in various pages, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24594**	https://plugins.trac.wordpress.org/changeset/2607480/	A-GTR-GOOG-181121/220
gvectors					
wpdiscuz					
Cross-Site Request Forgery (CSRF)	08-Nov-21	4.3	The wpDiscuz WordPress plugin before 7.3.4 does check for CSRF when adding, editing and deleting	N/A	A-GVE-WPDI-181121/221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			comments, which could allow attacker to make logged in users such as admin edit and delete arbitrary comment, or the user who made the comment to edit it via a CSRF attack. Attackers could also make logged in users post arbitrary comment. **CVE ID : CVE-2021-24806**		
g_auto-hyperlink_project					
g_auto-hyperlink					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	6.5	The G Auto-Hyperlink WordPress plugin through 1.0.1 does not sanitise or escape an 'id' GET parameter before using it in a SQL statement, to select data to be displayed in the admin dashboard, leading to an authenticated SQL injection **CVE ID : CVE-2021-24627**	N/A	A-G_A-G_AU-181121/222
hangfire					
hangfire					
Missing Authorization	02-Nov-21	5	Hangfire is an open source system to perform background job processing in a .NET or .NET Core applications. No Windows Service or separate process required. Dashboard UI in Hangfire.Core uses authorization filters to protect it from showing sensitive data to	https://github.com/HangfireIO/Hangfire/security/advisories/GHSA-7rq6-7gv8-c37h	A-HAN-HANG-181121/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized users. By default when no custom authorization filters specified, `LocalRequestsOnlyAuthorizationFilter` filter is being used to allow only local requests and prohibit all the remote requests to provide sensible, protected by default settings. However due to the recent changes, in version 1.7.25 no authorization filters are used by default, allowing remote requests to succeed. If you are using `UseHangfireDashboard` method with default `DashboardOptions.Authorization` property value, then your installation is impacted. If any other authorization filter is specified in the `DashboardOptions.Authorization` property, the you are not impacted. Patched versions (1.7.26) are available both on Nuget.org and as a tagged release on the github repo. Default authorization rules now prohibit remote requests by default again by including the `LocalRequestsOnlyAuthorizationFilter` filter to the default settings. Please upgrade to the newest version in order to mitigate		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the issue. For users who are unable to upgrade it is possible to mitigate the issue by using the `LocalRequestsOnlyAuthorizationFilter` explicitly when configuring the Dashboard UI. **CVE ID : CVE-2021-41238**		
hashthemes					
hashthemes_demo_importer					
Improper Access Control	01-Nov-21	5.5	The Hashthemes Demo Importer Plugin <= 1.1.1 for WordPress contained several AJAX functions which relied on a nonce which was visible to all logged-in users for access control, allowing them to execute a function that truncated nearly all database tables and removed the contents of wp-content/uploads. **CVE ID : CVE-2021-39333**	N/A	A-HAS-HASH-181121/224
Hitachi					
vantara_pentaho					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	7.5	Hitachi Vantara Pentaho Business Analytics through 9.1 allows an unauthenticated user to execute arbitrary SQL queries on any Pentaho data source and thus retrieve data from the related databases, as demonstrated by an api/repos/dashboards/edit	https://www.hitachi.com/hirt/security/index.html	A-HIT-VANT-181121/225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or URI. **CVE ID : CVE-2021-34684**		
Unrestricted Upload of File with Dangerous Type	08-Nov-21	6.5	UploadService in Hitachi Vantara Pentaho Business Analytics through 9.1 does not properly verify uploaded user files, which allows an authenticated user to upload various files of different file types. Specifically, a .jsp file is not allowed, but a .jsp. file is allowed (and leads to remote code execution). **CVE ID : CVE-2021-34685**	https://www.hitachi.com/hirt/security/index.html	A-HIT-VANT-181121/226
Unrestricted Upload of File with Dangerous Type	08-Nov-21	6.5	An issue was discovered in Hitachi Vantara Pentaho through 9.1 and Pentaho Business Intelligence Server through 7.x. A reports (.prpt) file allows the inclusion of BeanShell scripts to ease the production of complex reports. An authenticated user can run arbitrary code. **CVE ID : CVE-2021-31599**	https://www.hitachi.com/hirt/security/index.html	A-HIT-VANT-181121/227
Files or Directories Accessible to External Parties	08-Nov-21	4	An issue was discovered in Hitachi Vantara Pentaho through 9.1 and Pentaho Business Intelligence Server through 7.x. They implement a series of web services using the SOAP protocol to allow scripting interaction with the backend server. An authenticated user (regardless of privileges)	https://www.hitachi.com/hirt/security/index.html	A-HIT-VANT-181121/228

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
			can list all valid usernames. **CVE ID : CVE-2021-31600**		
Incorrect Authorization	08-Nov-21	4	An issue was discovered in Hitachi Vantara Pentaho through 9.1 and Pentaho Business Intelligence Server through 7.x. They implement a series of web services using the SOAP protocol to allow scripting interaction with the backend server. An authenticated user (regardless of privileges) can list all databases connection details and credentials. **CVE ID : CVE-2021-31601**	https://www.hitachi.com/hirt/security/index.html	A-HIT-VANT-181121/229
Incorrect Authorization	08-Nov-21	5	An issue was discovered in Hitachi Vantara Pentaho through 9.1 and Pentaho Business Intelligence Server through 7.x. The Security Model has different layers of Access Control. One of these layers is the applicationContext security, which is defined in the applicationContext-spring-security.xml file. The default configuration allows an unauthenticated user with no previous knowledge of the platform settings to extract pieces of information without possessing valid credentials. **CVE ID : CVE-2021-31602**	https://www.hitachi.com/hirt/security/index.html	A-HIT-VANT-181121/230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vantara_pentaho_business_intelligence_server					
Unrestricted Upload of File with Dangerous Type	08-Nov-21	6.5	An issue was discovered in Hitachi Vantara Pentaho through 9.1 and Pentaho Business Intelligence Server through 7.x. A reports (.prpt) file allows the inclusion of BeanShell scripts to ease the production of complex reports. An authenticated user can run arbitrary code. **CVE ID : CVE-2021-31599**	https://www.hitachi.com/hirt/security/index.html	A-HIT-VANT-181121/231
Files or Directories Accessible to External Parties	08-Nov-21	4	An issue was discovered in Hitachi Vantara Pentaho through 9.1 and Pentaho Business Intelligence Server through 7.x. They implement a series of web services using the SOAP protocol to allow scripting interaction with the backend server. An authenticated user (regardless of privileges) can list all valid usernames. **CVE ID : CVE-2021-31600**	https://www.hitachi.com/hirt/security/index.html	A-HIT-VANT-181121/232
Incorrect Authorization	08-Nov-21	4	An issue was discovered in Hitachi Vantara Pentaho through 9.1 and Pentaho Business Intelligence Server through 7.x. They implement a series of web services using the SOAP protocol to allow scripting interaction with the backend server. An authenticated user (regardless of privileges)	https://www.hitachi.com/hirt/security/index.html	A-HIT-VANT-181121/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can list all databases connection details and credentials. **CVE ID : CVE-2021-31601**		
Incorrect Authorization	08-Nov-21	5	An issue was discovered in Hitachi Vantara Pentaho through 9.1 and Pentaho Business Intelligence Server through 7.x. The Security Model has different layers of Access Control. One of these layers is the applicationContext security, which is defined in the applicationContext-spring-security.xml file. The default configuration allows an unauthenticated user with no previous knowledge of the platform settings to extract pieces of information without possessing valid credentials. **CVE ID : CVE-2021-31602**	https://www.hitachi.com/hirt/security/index.html	A-HIT-VANT-181121/234
hospital_management_system_project					
hospital_management_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-21	4.3	Multiple Cross Site Scripting (XSS) vulnerabilities exist in PHPGurukul Hospital Management System 4.0 via the (1) searchdata parameter in (a) doctor/search.php and (b) admin/patient-search.php, and the (2) fromdate and (3) todate parameters in admin/betweendates-detailsreports.php.	N/A	A-HOS-HOSP-181121/235

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
			CVE ID : CVE-2021-39411		
HP					
hp_smart					
Improper Privilege Management	01-Nov-21	4.6	HP Print and Scan Doctor, an application within the HP Smart App for Windows, is potentially vulnerable to local elevation of privilege. **CVE ID : CVE-2021-3440**	https://support.hp.com/us-en/document/ish_4120228-4120263-16/hpsbpi03727	A-HP-HP_S-181121/236
ilo_amplifier_pack					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Nov-21	10	A remote unauthenticated directory traversal security vulnerability has been identified in HPE iLO Amplifier Pack versions 1.80, 1.81, 1.90 and 1.95. The vulnerability could be remotely exploited to allow an unauthenticated user to run arbitrary code leading complete impact to confidentiality, integrity, and availability of the iLO Amplifier Pack appliance. **CVE ID : CVE-2021-29212**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn04189en_us	A-HP-ILO_-181121/237
htmldoc_project					
htmldoc					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Nov-21	4.3	Buffer overflow vulnerability in htmldoc before 1.9.12, allows attackers to cause a denial of service via a crafted BMP image to image_load_bmp. **CVE ID : CVE-2021-40985**	https://github.com/michaelrsweet/htmldoc/commit/f12b9666e582a8e7b70f11b28e5ffc49ad62	A-HTM-HTML-181121/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				5d43, https://github.com/michaelrsweet/htmldoc/issues/444	
IBM					
business_automation_workflow					
Cleartext Transmission of Sensitive Information	05-Nov-21	4.3	IBM Business Automation Workflow 18. 19, 20, 21, and IBM Business Process Manager 8.5 and d8.6 transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. **CVE ID : CVE-2021-29753**	https://www.ibm.com/support/pages/node/6513703, https://exchange.xforce.ibmcloud.com/vulnerabilities/201919	A-IBM-BUSI-181121/239
business_process_manager					
Cleartext Transmission of Sensitive Information	05-Nov-21	4.3	IBM Business Automation Workflow 18. 19, 20, 21, and IBM Business Process Manager 8.5 and d8.6 transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. **CVE ID : CVE-2021-29753**	https://www.ibm.com/support/pages/node/6513703, https://exchange.xforce.ibmcloud.com/vulnerabilities/201919	A-IBM-BUSI-181121/240
infosphere_information_server					
Exposure of Sensitive Information to an	10-Nov-21	4	IBM InfoSphere Information Server 11.7 could allow an authenticated user to obtain sensitive information from	https://www.ibm.com/support/pages/node/651	A-IBM-INFO-181121/241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			application response requests that could be used in further attacks against the system. IBM X-Force ID: 209401. **CVE ID : CVE-2021-38887**	0178, https://exchange.xforce.ibmcloud.com/vulnerabilities/209401	
XML Injection (aka Blind XPath Injection)	02-Nov-21	6.4	IBM InfoSphere Information Server 11.7 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 211402. **CVE ID : CVE-2021-38948**	https://www.ibm.com/support/pages/node/6509632, https://exchange.xforce.ibmcloud.com/vulnerabilities/211402	A-IBM-INFO-181121/242
Improper Certificate Validation	02-Nov-21	5	IBM InfoSphere Data Flow Designer Engine (IBM InfoSphere Information Server 11.7) component has improper validation of the REST API server certificate. IBM X-Force ID: 201301. **CVE ID : CVE-2021-29737**	https://exchange.xforce.ibmcloud.com/vulnerabilities/201301, https://www.ibm.com/support/pages/node/6509086	A-IBM-INFO-181121/243
Server-Side Request Forgery (SSRF)	02-Nov-21	5.5	IBM InfoSphere Data Flow Designer (IBM InfoSphere Information Server 11.7) 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	https://exchange.xforce.ibmcloud.com/vulnerabilities/201302, https://www.ibm.com/support/pages/node/650	A-IBM-INFO-181121/244

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
			enumeration or facilitating other attacks. IBM X-Force ID: 201302. **CVE ID : CVE-2021-29738**	9084	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-21	3.5	IBM InfoSphere Information Server 11.7 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. **CVE ID : CVE-2021-29771**	https://www.ibm.com/support/pages/node/6509614, https://exchange.xforce.ibmcloud.com/vulnerabilities/202773	A-IBM-INFO-181121/245
N/A	02-Nov-21	5	IBM InfoSphere Information Server 11.7 could allow an attacker to obtain sensitive information due to a insecure third party domain access vulnerability. IBM X-Force ID: 206572. **CVE ID : CVE-2021-29875**	https://exchange.xforce.ibmcloud.com/vulnerabilities/206572, https://www.ibm.com/support/pages/node/6509616	A-IBM-INFO-181121/246
Cross-Site Request Forgery (CSRF)	02-Nov-21	6.8	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 207123. **CVE ID : CVE-2021-29888**	https://exchange.xforce.ibmcloud.com/vulnerabilities/207123, https://www.ibm.com/support/pages/node/6509618	A-IBM-INFO-181121/247
mq_appliance					

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
N/A	08-Nov-21	4	IBM MQ 9.1 LTS, 9.1 CD, 9.2 LTS, and 9.2CD is vulnerable to a denial of service attack caused by an issue processing message properties. IBM X-Force ID: 205203. **CVE ID : CVE-2021-29843**	https://exchange.xforce.ibmcloud.com/vulnerabilities/205203, https://www.ibm.com/support/pages/node/6513681	A-IBM-MQ_A-181121/248
security_guardium					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	3.5	IBM Security Guardium 10.5, 10.6, 11.0, 11.1, 11.2, and 11.3 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. **CVE ID : CVE-2021-29735**	https://www.ibm.com/support/pages/node/6514007, https://exchange.xforce.ibmcloud.com/vulnerabilities/201239	A-IBM-SECU-181121/249
igexsolutions					
wpschoolpress					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	6.5	The School Management System â€“ WPSchoolPress WordPress plugin before 2.1.10 does not properly sanitize or use prepared statements before using POST variable in SQL queries, leading to SQL injection in multiple actions available to various authenticated users, from simple	N/A	A-IGE-WPSC-181121/250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subscribers/students to teachers and above. **CVE ID : CVE-2021-24575**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	3.5	The School Management System â€“ WPSchoolPress WordPress plugin before 2.1.17 sanitise some fields using sanitize_text_field() but does not escape them before outputting in attributes, resulting in Stored Cross-Site Scripting issues. **CVE ID : CVE-2021-24664**	N/A	A-IGE-WPSC-181121/251
imagesourcecontrol					
image_source_control					
N/A	01-Nov-21	4	The Image Source Control WordPress plugin before 2.3.1 allows users with a role as low as Contributor to change arbitrary post meta fields of arbitrary posts (even those they should not be able to edit) **CVE ID : CVE-2021-24781**	https://plugins.trac.wordpress.org/changeset/2606615/	A-IMA-IMAG-181121/252
jeedom					
jeedom					
Insufficiently Protected Credentials	01-Nov-21	5	In Jeedom through 4.1.19, a bug allows a remote attacker to bypass API access and retrieve users credentials. **CVE ID : CVE-2021-42557**	N/A	A-JEE-JEED-181121/253
Jenkins					
jenkins					
Missing	04-Nov-21	6.4	Jenkins 2.318 and earlier,	https://ww	A-JEN-JENK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			LTS 2.303.2 and earlier does not check agent-to-controller access to create parent directories in FilePath#mkdirs. **CVE ID : CVE-2021-21685**	w.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455	181121/254
Improper Link Resolution Before File Access ('Link Following')	04-Nov-21	5.8	File path filters in the agent-to-controller security subsystem of Jenkins 2.318 and earlier, LTS 2.303.2 and earlier do not canonicalize paths, allowing operations to follow symbolic links to outside allowed directories. **CVE ID : CVE-2021-21686**	https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455	A-JEN-JENK-181121/255
Missing Authorization	04-Nov-21	6.4	Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not check agent-to-controller access to create symbolic links when unarchiving a symbolic link in FilePath#untar. **CVE ID : CVE-2021-21687**	https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455	A-JEN-JENK-181121/256
Missing Authorization	04-Nov-21	5	The agent-to-controller security check FilePath#reading(FileVisitor) in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not reject any operations, allowing users to have unrestricted read access using certain operations (creating archives, FilePath#copyRecursiveTo). **CVE ID : CVE-2021-21688**	https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455	A-JEN-JENK-181121/257
Missing Authorizatio	04-Nov-21	6.4	FilePath#unzip and FilePath#untar were not	https://www.jenkins.io/	A-JEN-JENK-

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
n			subject to any agent-to-controller access control in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier. **CVE ID : CVE-2021-21689**	security/advisory/2021-11-04/#SECURITY-2455	181121/258
Protection Mechanism Failure	04-Nov-21	7.5	Agent processes are able to completely bypass file path filtering by wrapping the file operation in an agent file path in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier. **CVE ID : CVE-2021-21690**	https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455	A-JEN-JENK-181121/259
Incorrect Authorization	04-Nov-21	7.5	Creating symbolic links is possible without the 'symlink' agent-to-controller access control permission in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier. **CVE ID : CVE-2021-21691**	https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455	A-JEN-JENK-181121/260
Incorrect Authorization	04-Nov-21	7.5	FilePath#renameTo and FilePath#moveAllChildrenTo in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier only check 'read' agent-to-controller access permission on the source path, instead of 'delete'. **CVE ID : CVE-2021-21692**	https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455	A-JEN-JENK-181121/261
Improper Authorization	04-Nov-21	7.5	When creating temporary files, agent-to-controller access to create those files is only checked after they've been created in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier. **CVE ID : CVE-2021-21693**	https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455	A-JEN-JENK-181121/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	04-Nov-21	7.5	FilePath#toURI, FilePath#hasSymlink, FilePath#absolutize, FilePath#isDescendant, and FilePath#get*DiskSpace do not check any permissions in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier. **CVE ID : CVE-2021-21694**	https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455	A-JEN-JENK-181121/263
Missing Authorization	04-Nov-21	6.8	FilePath#listFiles lists files outside directories that agents are allowed to access when following symbolic links in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier. **CVE ID : CVE-2021-21695**	https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455	A-JEN-JENK-181121/264
Protection Mechanism Failure	04-Nov-21	7.5	Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not limit agent read/write access to the libs/ directory inside build directories when using the FilePath APIs, allowing attackers in control of agent processes to replace the code of a trusted library with a modified variant. This results in unsandboxed code execution in the Jenkins controller process. **CVE ID : CVE-2021-21696**	https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2423	A-JEN-JENK-181121/265
Incomplete List of Disallowed Inputs	04-Nov-21	6.4	Jenkins 2.318 and earlier, LTS 2.303.2 and earlier allows any agent to read and write the contents of any build directory stored in Jenkins with very few restrictions.	https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2428	A-JEN-JENK-181121/266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21697		
subversion					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Nov-21	5	Jenkins Subversion Plugin 2.15.0 and earlier does not restrict the name of a file when looking up a subversion key file on the controller from an agent. **CVE ID : CVE-2021-21698**	https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2506	A-JEN-SUBV-181121/267
Jetbrains					
hub					
N/A	09-Nov-21	5	In JetBrains Hub before 2021.1.13690, information disclosure via avatar metadata is possible. **CVE ID : CVE-2021-43180**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-HUB-181121/268
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-21	4.3	In JetBrains Hub before 2021.1.13690, stored XSS is possible. **CVE ID : CVE-2021-43181**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-HUB-181121/269
N/A	09-Nov-21	5	In JetBrains Hub before 2021.1.13415, a DoS via user information is possible. **CVE ID : CVE-2021-43182**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-HUB-181121/270
Improper Authenticati	09-Nov-21	7.5	In JetBrains Hub before 2021.1.13690, the	https://blog.jetbrains.co	A-JET-HUB-181121/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			authentication throttling mechanism could be bypassed. **CVE ID : CVE-2021-43183**	m/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	
ktor					
Improper Authentication	09-Nov-21	5	In JetBrains Ktor before 1.6.4, nonce verification during the OAuth2 authentication process is implemented improperly. **CVE ID : CVE-2021-43203**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-KTOR-181121/272
teamcity					
N/A	09-Nov-21	7.5	In JetBrains TeamCity before 2021.1.2, remote code execution via the agent push functionality is possible. **CVE ID : CVE-2021-43193**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-TEAM-181121/273
N/A	09-Nov-21	5	In JetBrains TeamCity before 2021.1.2, user enumeration was possible. **CVE ID : CVE-2021-43194**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-TEAM-181121/274
N/A	09-Nov-21	5	In JetBrains TeamCity before 2021.1.2, some HTTP security headers were missing. **CVE ID : CVE-2021-43195**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-	A-JET-TEAM-181121/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021/	
Exposure of Resource to Wrong Sphere	09-Nov-21	5	In JetBrains TeamCity before 2021.1, information disclosure via the Docker Registry connection dialog is possible. **CVE ID : CVE-2021-43196**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-TEAM-181121/276
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-21	4.3	In JetBrains TeamCity before 2021.1.2, email notifications could include unescaped HTML for XSS. **CVE ID : CVE-2021-43197**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-TEAM-181121/277
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-21	3.5	In JetBrains TeamCity before 2021.1.2, stored XSS is possible. **CVE ID : CVE-2021-43198**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-TEAM-181121/278
Incorrect Default Permissions	09-Nov-21	5	In JetBrains TeamCity before 2021.1.2, permission checks in the Create Patch functionality are insufficient. **CVE ID : CVE-2021-43199**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-TEAM-181121/279
N/A	09-Nov-21	7.5	In JetBrains TeamCity before 2021.1.2, permission checks in the Agent Push functionality were insufficient. **CVE ID : CVE-2021-43200**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-	A-JET-TEAM-181121/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				bulletin-q3-2021/	
N/A	09-Nov-21	5	In JetBrains TeamCity before 2021.1.3, a newly created project could take settings from an already deleted project. **CVE ID : CVE-2021-43201**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-TEAM-181121/281
youtrack					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-21	3.5	In JetBrains YouTrack before 2021.3.21051, stored XSS is possible. **CVE ID : CVE-2021-43184**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-YOUT-181121/282
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-Nov-21	7.5	JetBrains YouTrack before 2021.3.23639 is vulnerable to Host header injection. **CVE ID : CVE-2021-43185**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-YOUT-181121/283
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-21	3.5	JetBrains YouTrack before 2021.3.24402 is vulnerable to stored XSS. **CVE ID : CVE-2021-43186**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-YOUT-181121/284
youtrack_mobile					
N/A	09-Nov-21	5	In JetBrains YouTrack Mobile before 2021.2, the	https://blog.jetbrains.co	A-JET-YOUT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client-side cache on iOS could contain sensitive information. **CVE ID : CVE-2021-43187**	m/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	181121/285
N/A	09-Nov-21	5	In JetBrains YouTrack Mobile before 2021.2, task hijacking on Android is possible. **CVE ID : CVE-2021-43190**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-YOUT-181121/286
N/A	09-Nov-21	5	JetBrains YouTrack Mobile before 2021.2, is missing the security screen on Android and iOS. **CVE ID : CVE-2021-43191**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-YOUT-181121/287
N/A	09-Nov-21	5	In JetBrains YouTrack Mobile before 2021.2, iOS URL scheme hijacking is possible. **CVE ID : CVE-2021-43192**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	A-JET-YOUT-181121/288
json-ptr_project					
json-ptr					
Access of Resource Using Incompatible Type ('Type Confusion')	03-Nov-21	7.5	This affects the package json-ptr before 3.0.0. A type confusion vulnerability can lead to a bypass of CVE-2020-7766 when the user-provided keys used in the pointer parameter are	https://github.com/flitbit/json-ptr/commit/5dc458fbad1c382a2e3ca6d62e66ed	A-JSO-JSON-181121/289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arrays. **CVE ID : CVE-2021-23509**	e3d92849ca, https://snyk.io/vuln/SNYK-JS-JSONPTR-1577291, https://github.com/flitbit/json-ptr/pull/42, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1767165	
jsonpointer_project					
jsonpointer					
Access of Resource Using Incompatible Type ('Type Confusion')	03-Nov-21	7.5	This affects the package jsonpointer before 5.0.0. A type confusion vulnerability can lead to a bypass of a previous Prototype Pollution fix when the pointer components are arrays. **CVE ID : CVE-2021-23807**	https://snyk.io/vuln/SNYK-JS-JSONPOINTER-1577288, https://github.com/janl/node-jsonpointer/pull/51, https://github.com/janl/node-jsonpointer/commit/a0345f3550cd9c4d89f33b126390202b89510ad4, https://snyk.io/vuln/SNYK-JAVA-	A-JSO-JSON-181121/290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ORGWEBJARSNPM-1910273	
Access of Resource Using Incompatible Type ('Type Confusion')	03-Nov-21	7.5	This affects all versions of package json-pointer. A type confusion vulnerability can lead to a bypass of CVE-2020-7709 when the pointer components are arrays. **CVE ID : CVE-2021-23820**	https://snyk.io/vuln/SNYK-JS-JSONPOINTER-1577287, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1910686	A-JSO-JSON-181121/291
Jupyter					
jupyterhub					
Insufficient Session Expiration	04-Nov-21	5	JupyterHub is an open source multi-user server for Jupyter notebooks. In affected versions users who have multiple JupyterLab tabs open in the same browser session, may see incomplete logout from the single-user server, as fresh credentials (for the single-user server only, not the Hub) reinstated after logout, if another active JupyterLab session is open while the logout takes place. Upgrade to JupyterHub 1.5. For distributed deployments, it is jupyterhub in the _user_ environment that needs patching. There are no patches necessary in the Hub environment. The only workaround is to make sure	https://github.com/jupyterhub/jupyterhub/security/advisories/GHSA-cw7p-q79f-m2v7, https://github.com/jupyterhub/jupyterhub/commit/5ac9e7f73a6e1020ffddc40321fc53336829fe27	A-JUP-JUPY-181121/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that only one JupyterLab tab is open when you log out. **CVE ID : CVE-2021-41247**		
nbdime					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-21	3.5	nbdime provides tools for diffing and merging of Jupyter Notebooks. In affected versions a stored cross-site scripting (XSS) issue exists within the Jupyter-owned nbdime project. It appears that when reading the file name and path from disk, the extension does not sanitize the string it constructs before returning it to be displayed. The diffNotebookCheckpoint function within nbdime causes this issue. When attempting to display the name of the local notebook (diffNotebookCheckpoint), nbdime appears to simply append .ipynb to the name of the input file. The NbdimeWidget is then created, and the base string is passed through to the request API function. From there, the frontend simply renders the HTML tag and anything along with it. Users are advised to patch to the most recent version of the affected product. **CVE ID : CVE-2021-41134**	https://github.com/jupyter/nbdime/commit/e44a5cc7677f24b45ebafc756db49058c2f750ea, https://github.com/jupyter/nbdime/security/advisories/GHSA-p6rw-44q7-3fw4	A-JUP-NBDI-181121/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nbdime-jupyterlab					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-21	3.5	nbdime provides tools for diffing and merging of Jupyter Notebooks. In affected versions a stored cross-site scripting (XSS) issue exists within the Jupyter-owned nbdime project. It appears that when reading the file name and path from disk, the extension does not sanitize the string it constructs before returning it to be displayed. The diffNotebookCheckpoint function within nbdime causes this issue. When attempting to display the name of the local notebook (diffNotebookCheckpoint), nbdime appears to simply append .ipynb to the name of the input file. The NbdimeWidget is then created, and the base string is passed through to the request API function. From there, the frontend simply renders the HTML tag and anything along with it. Users are advised to patch to the most recent version of the affected product. **CVE ID : CVE-2021-41134**	https://github.com/jupyter/nbdime/commit/e44a5cc7677f24b45ebafc756db49058c2f750ea, https://github.com/jupyter/nbdime/security/advisories/GHSA-p6rw-44q7-3fw4	A-JUP-NBDI-181121/294
Kaspersky					
endpoint_security					
N/A	03-Nov-21	7.8	Possible system denial of service in case of arbitrary	N/A	A-KAS-ENDP-181121/295

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
			changing Firefox browser parameters. An attacker could change specific Firefox browser parameters file in a certain way and then reboot the system to make the system unbootable. **CVE ID : CVE-2021-35053**		
kaysongroup					
php_event_calendar					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	10	PHP Event Calendar before 2021-09-03 allows SQL injection, as demonstrated by the /server/ajax/user_manager.php username parameter. This can be used to execute SQL statements directly on the database, allowing an adversary in some cases to completely compromise the database system. It can also be used to bypass the login form. **CVE ID : CVE-2021-42077**	N/A	A-KAY-PHP_-181121/296
Kodi					
kodi					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Nov-21	4.3	Buffer overflow vulnerability in Kodi xbmc up to 19.0, allows attackers to cause a denial of service due to improper length of values passed to istream. **CVE ID : CVE-2021-42917**	https://github.com/xbmc/xbmc/pull/20306, https://github.com/fuzzard/xbmc/commit/80c8138c09598e88b4ddb6db	A-KOD-KODI-181121/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				b279fa193bbb3237, https://github.com/xbmc/xbmc/commit/48730b64494798705d46dfccc4029bd36d072df3	
legalweb					
wp_dsgvo_tools					
Missing Authorization	05-Nov-21	6.4	WP DSGVO Tools (GDPR) <= 3.1.23 had an AJAX action, ‘admin-dismiss-unsubscribe‘, which lacked a capability check and a nonce check and was available to unauthenticated users, and did not check the post type when deleting unsubscription requests. As such, it was possible for an attacker to permanently delete an arbitrary post or page on the site by sending an AJAX request with the “action” parameter set to “admin-dismiss-unsubscribe” and the “id” parameter set to the post to be deleted. Sending such a request would move the post to the trash, and repeating the request would permanently delete the post in question. **CVE ID : CVE-2021-42359**	N/A	A-LEG-WP_D-181121/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
libjxl_project					
libjxl					
Out-of-bounds Read	01-Nov-21	3.6	Invalid JPEG XL images using libjxl can cause an out of bounds access on a std::vector<std::vector<T>> when rendering splines. The OOB read access can either lead to a segfault, or rendering splines based on other process memory. It is recommended to upgrade past 0.6.0 or patch with https://github.com/libjxl/libjxl/pull/757 **CVE ID : CVE-2021-22563**	https://github.com/libjxl/libjxl/issues/735, https://github.com/libjxl/libjxl/pull/757	A-LIB-LIBJ-181121/299
Out-of-bounds Write	01-Nov-21	2.1	For certain valid JPEG XL images with a size slightly larger than an integer number of groups (256x256 pixels) when processing the groups out of order the decoder can perform an out of bounds copy of image pixels from an image buffer in the heap to another. This copy can occur when processing the right or bottom edges of the image, but only when groups are processed in certain order. Groups can be processed out of order in multi-threaded decoding environments with heavy thread load but also with images that contain the groups in an arbitrary order in the file. It is recommended to upgrade	https://github.com/libjxl/libjxl/pull/775, https://github.com/libjxl/libjxl/issues/708	A-LIB-LIBJ-181121/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			past 0.6.0 or patch with https://github.com/libjxl/libjxl/pull/775 **CVE ID : CVE-2021-22564**		
librenms					
librenms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-21	4.3	LibreNMS through 21.10.2 allows XSS via a widget title. **CVE ID : CVE-2021-43324**	https://github.com/librenms/librenms/commit/99d2462b80435b91a35236639b909eebee432126	A-LIB-LIBR-181121/301
libxls_project					
libxls					
NULL Pointer Dereference	03-Nov-21	4.3	An issue was discoverered in in function xls_getWorkSheet in xls.c in libxls 1.6.2, allows attackers to cause a denial of service, via a crafted XLS file. **CVE ID : CVE-2021-27836**	https://github.com/libxls/libxls/issues/94	A-LIB-LIBX-181121/302
llhttp					
llhttp					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	03-Nov-21	5.8	The parse function in llhttp < 2.1.4 and < 6.0.6. ignores chunk extensions when parsing the body of chunked requests. This leads to HTTP Request Smuggling (HRS) under certain conditions. **CVE ID : CVE-2021-22960**	N/A	A-LLH-LLHT-181121/303
loco_translate_project					
loco_translate					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	08-Nov-21	4	The Loco Translate WordPress plugin before 2.5.4 mishandles data inputs which get saved to a file, which can be renamed to an extension ending in .php, resulting in authenticated "translator" users being able to inject PHP code into files ending with .php in web accessible locations. **CVE ID : CVE-2021-24721**	N/A	A-LOC-LOCO-181121/304
LUA					
lua					
Out-of-bounds Write	09-Nov-21	4.3	Stack overflow in lua_resume of ldo.c in Lua Interpreter 5.1.0~5.4.4 allows attackers to perform a Denial of Service via a crafted script file. **CVE ID : CVE-2021-43519**	http://lua-users.org/lists/lua-l/2021-11/msg00015.html, http://lua-users.org/lists/lua-l/2021-10/msg00123.html	A-LUA-LUA-181121/305
Mahara					
mahara					
Improper Neutralization of Formula Elements in a CSV File	03-Nov-21	6.8	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, exported CSV files could contain characters that a spreadsheet program could interpret as a command, leading to execution of a malicious string locally on a device,	https://mahara.org/interaction/forum/topic.php?id=8950, https://bugs.launchpad.net/mahara/+bug/19304	A-MAH-MAHA-181121/306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka CSV injection. **CVE ID : CVE-2021-40848**	71	
Insufficient Session Expiration	03-Nov-21	7.5	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, the account associated with a web services token is vulnerable to being exploited and logged into, resulting in information disclosure (at a minimum) and often escalation of privileges. **CVE ID : CVE-2021-40849**	https://mahara.org/interaction/forum/topic.php?id=8949, https://bugs.launchpad.net/mahara/+bug/1930469	A-MAH-MAHA-181121/307
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Nov-21	2.1	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, adjusting the path component for the page help file allows attackers to bypass the intended access control for HTML files via directory traversal. It replaces the - character with the / character. **CVE ID : CVE-2021-43264**	https://mahara.org/interaction/forum/topic.php?id=8954	A-MAH-MAHA-181121/308
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-21	3.5	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, certain tag syntax could be used for XSS, such as via a SCRIPT element. **CVE ID : CVE-2021-43265**	https://mahara.org/interaction/forum/topic.php?id=8953	A-MAH-MAHA-181121/309
Improper Neutralization of Special Elements used in a Command ('Command	02-Nov-21	4.6	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, exporting collections via PDF export could lead to code execution via shell metacharacters in a collection name.	https://mahara.org/interaction/forum/topic.php?id=8952	A-MAH-MAHA-181121/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			**CVE ID : CVE-2021-43266**		
Mcafee					
data_loss_prevention_endpoint					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	3.5	Cross site scripting (XSS) vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.7.100 allows a remote attacker to highjack an active DLP ePO administrator session by convincing the logged in administrator to click on a carefully crafted link in the case management part of the DLP ePO extension. **CVE ID : CVE-2021-31848**	https://kc.mcafee.com/corporate/index?page=content&id=SB10371	A-MCA-DATA-181121/311
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-21	6.5	SQL injection vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.7.100 allows a remote attacker logged into ePO as an administrator to inject arbitrary SQL into the ePO database through the user management section of the DLP ePO extension. **CVE ID : CVE-2021-31849**	https://kc.mcafee.com/corporate/index?page=content&id=SB10371	A-MCA-DATA-181121/312
drive_encryption					
Uncontrolled Search Path Element	10-Nov-21	4.6	DLL Search Order Hijacking Vulnerability in McAfee Drive Encryption (MDE) prior to 7.3.0 HF2 (7.3.0.183) allows local users to execute arbitrary code and escalate privileges via execution from a	https://kc.mcafee.com/corporate/index?page=content&id=SB10374	A-MCA-DRIV-181121/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compromised folder. **CVE ID : CVE-2021-31853**		
mendix					
mendix					
Use of Web Browser Cache Containing Sensitive Information	09-Nov-21	1.9	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.26), Mendix Applications using Mendix 8 (All versions < V8.18.12), Mendix Applications using Mendix 9 (All versions < V9.6.1). Applications built with affected versions of Mendix Studio Pro do not prevent file documents from being cached when files are opened or downloaded using a browser. This could allow a local attacker to read those documents by exploring the browser cache. **CVE ID : CVE-2021-42015**	https://cert-portal.siemens.com/productcert/pdf/ssa-338732.pdf	A-MEN-MEND-181121/314
Incorrect Authorization	09-Nov-21	6.8	A vulnerability has been identified in Mendix Applications using Mendix 8 (All versions < V8.18.13), Mendix Applications using Mendix 9 (All versions < V9.6.2). Applications built with affected versions of Mendix Studio Pro do not properly control write access for certain client actions. This could allow authenticated attackers to manipulate the content of	https://cert-portal.siemens.com/productcert/pdf/ssa-779699.pdf	A-MEN-MEND-181121/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			System.FileDocument objects in some cases, regardless whether they have write access to it. **CVE ID : CVE-2021-42025**		
Incorrect Authorization	09-Nov-21	4	A vulnerability has been identified in Mendix Applications using Mendix 8 (All versions < V8.18.13), Mendix Applications using Mendix 9 (All versions < V9.6.2). Applications built with affected versions of Mendix Studio Pro do not properly control read access for certain client actions. This could allow authenticated attackers to retrieve the changedDate attribute of arbitrary objects, even when they don't have read access to them. **CVE ID : CVE-2021-42026**	https://cert-portal.siemens.com/productcert/pdf/ssa-779699.pdf	A-MEN-MEND-181121/316
Microsoft					
365_apps					
N/A	10-Nov-21	6.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2021-40442**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40442	A-MIC-365_-181121/317
N/A	10-Nov-21	6.8	Microsoft Access Remote Code Execution Vulnerability **CVE ID : CVE-2021-41368**	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-365_-181121/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2021-41368	
Incorrect Authorization	10-Nov-21	6.8	Microsoft Excel Security Feature Bypass Vulnerability **CVE ID : CVE-2021-42292**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42292	A-MIC-365_-181121/319
Improper Control of Generation of Code ('Code Injection')	10-Nov-21	6.9	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2021-42296**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42296	A-MIC-365_-181121/320
azure_real_time_operating_system					
N/A	10-Nov-21	1.9	Azure RTOS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-42301, CVE-2021-42323. **CVE ID : CVE-2021-26444**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26444	A-MIC-AZUR-181121/321
azure_sphere					
N/A	10-Nov-21	2.1	Azure Sphere Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-41375, CVE-2021-41376. **CVE ID : CVE-2021-41374**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41374	A-MIC-AZUR-181121/322
N/A	10-Nov-21	2.1	Azure Sphere Information Disclosure Vulnerability	https://portal.msrc.micr	A-MIC-AZUR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2021-41374, CVE-2021-41376. **CVE ID : CVE-2021-41375**	osoft.com/en-US/security-guidance/advisory/CVE-2021-41375	181121/323
N/A	10-Nov-21	2.1	Azure Sphere Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-41374, CVE-2021-41375. **CVE ID : CVE-2021-41376**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41376	A-MIC-AZUR-181121/324
edge					
N/A	10-Nov-21	4.3	Microsoft Edge (Chrome based) Spoofing on IE Mode **CVE ID : CVE-2021-41351**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41351	A-MIC-EDGE-181121/325
excel					
N/A	10-Nov-21	6.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2021-40442**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40442	A-MIC-EXCE-181121/326
Incorrect Authorization	10-Nov-21	6.8	Microsoft Excel Security Feature Bypass Vulnerability **CVE ID : CVE-2021-42292**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	A-MIC-EXCE-181121/327

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
				2021-42292	
exchange_server					
N/A	10-Nov-21	4.3	Microsoft Exchange Server Spoofing Vulnerability This CVE ID is unique from CVE-2021-42305. **CVE ID : CVE-2021-41349**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41349	A-MIC-EXCH-181121/328
N/A	10-Nov-21	6.5	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2021-42321**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42321	A-MIC-EXCH-181121/329
fslogix					
N/A	10-Nov-21	2.1	FSLogix Information Disclosure Vulnerability **CVE ID : CVE-2021-41373**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41373	A-MIC-FSLO-181121/330
office					
N/A	10-Nov-21	6.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2021-40442**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40442	A-MIC-OFFI-181121/331
N/A	10-Nov-21	6.8	Microsoft Access Remote Code Execution	https://portal.msrc.micr	A-MIC-OFFI-181121/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability **CVE ID : CVE-2021-41368**	osoft.com/en-US/security-guidance/advisory/CVE-2021-41368	
Incorrect Authorization	10-Nov-21	6.8	Microsoft Excel Security Feature Bypass Vulnerability **CVE ID : CVE-2021-42292**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42292	A-MIC-OFFI-181121/333
Improper Control of Generation of Code ('Code Injection')	10-Nov-21	6.9	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2021-42296**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42296	A-MIC-OFFI-181121/334
office_long_term_servicing_channel					
N/A	10-Nov-21	6.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2021-40442**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40442	A-MIC-OFFI-181121/335
N/A	10-Nov-21	6.8	Microsoft Access Remote Code Execution Vulnerability **CVE ID : CVE-2021-41368**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41368	A-MIC-OFFI-181121/336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	10-Nov-21	6.8	Microsoft Excel Security Feature Bypass Vulnerability **CVE ID : CVE-2021-42292**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42292	A-MIC-OFFI-181121/337
office_online_server					
N/A	10-Nov-21	6.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2021-40442**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40442	A-MIC-OFFI-181121/338
office_web_apps_server					
N/A	10-Nov-21	6.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2021-40442**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40442	A-MIC-OFFI-181121/339
power_bi_report_server					
Cross-Site Request Forgery (CSRF)	10-Nov-21	6.8	Power BI Report Server Spoofing Vulnerability **CVE ID : CVE-2021-41372**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41372	A-MIC-POWE-181121/340
remote_desktop					
N/A	10-Nov-21	4.3	Remote Desktop Protocol Client Information	https://portal.msrc.micr	A-MIC-REMO-181121/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2021-38665**	osoft.com/en-US/security-guidance/advisory/CVE-2021-38665	
sharepoint_enterprise_server					
N/A	10-Nov-21	6.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2021-40442**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40442	A-MIC-SHAR-181121/342
visual_studio					
Improper Privilege Management	10-Nov-21	4.6	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42277**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42277	A-MIC-VISU-181121/343
visual_studio_2017					
Improper Privilege Management	10-Nov-21	4.6	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42277**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42277	A-MIC-VISU-181121/344
visual_studio_2019					
Improper Privilege Management	10-Nov-21	4.6	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42277**	https://portal.msrc.microsoft.com/en-	A-MIC-VISU-181121/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				US/security-guidance/advisory/CVE-2021-42277	
miniftpd_project					
miniftpd					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Nov-21	4.6	A local buffer overflow vulnerability exists in the latest version of Miniftpd in ftpproto.c through the tmp variable, where a crafted payload can be sent to the affected function. **CVE ID : CVE-2021-42624**	N/A	A-MIN-MINI-181121/346
motopress					
restaurant_menu					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	3.5	The Restaurant Menu by MotoPress WordPress plugin before 2.4.2 does not properly sanitize or escape inputs when creating new menu items, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24722**	N/A	A-MOT-REST-181121/347
Mozilla					
firefox					
N/A	03-Nov-21	4.3	Mixed-content checks were unable to analyze opaque origins which led to some mixed content being loaded. This vulnerability affects Firefox < 92. **CVE ID : CVE-2021-38491**	https://www.mozilla.org/security/advisories/mfsa2021-38/, https://bugzilla.mozilla.o	A-MOZ-FIRE-181121/348

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
				rg/show_bug.cgi?id=1551886	
N/A	03-Nov-21	4.3	When delegating navigations to the operating system, Firefox would accept the `mk` scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. *This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 92, Thunderbird < 91.1, Thunderbird < 78.14, Firefox ESR < 78.14, and Firefox ESR < 91.1. **CVE ID : CVE-2021-38492**	https://www.mozilla.org/security/advisories/mfsa2021-41/, https://www.mozilla.org/security/advisories/mfsa2021-40/, https://www.mozilla.org/security/advisories/mfsa2021-42/, https://www.mozilla.org/security/advisories/mfsa2021-38/	A-MOZ-FIRE-181121/349
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Nov-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 91 and Firefox ESR 78.13. 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 ESR < 78.14, Thunderbird < 78.14, and Firefox < 92. **CVE ID : CVE-2021-38493**	https://www.mozilla.org/security/advisories/mfsa2021-42/, https://www.mozilla.org/security/advisories/mfsa2021-38/, https://www.mozilla.org/security/advisories/mfsa2021-39/, https://bugzilla.mozilla.o	A-MOZ-FIRE-181121/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				rg/buglist.cgi?bug_id=1723391%2C1724101%2C1724107	
N/A	03-Nov-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 91. 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 < 92. **CVE ID : CVE-2021-38494**	https://www.mozilla.org/security/advisories/mfsa2021-38/	A-MOZ-FIRE-181121/351
Use After Free	03-Nov-21	6.8	During operations on MessageTasks, a task may have been removed while it was still scheduled, resulting in memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR < 91.2, Firefox ESR < 78.15, and Firefox < 93. **CVE ID : CVE-2021-38496**	https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://www.mozilla.org/security/advisories/mfsa2021-44/, https://www.mozilla.org/security/advisories/mfsa2021-47/	A-MOZ-FIRE-181121/352
Origin Validation	03-Nov-21	4.3	Through use of reportValidity() and	https://www.mozilla.or	A-MOZ-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Error			window.open(), a plain-text validation message could have been overlaid on another origin, leading to possible user confusion and spoofing attacks. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2. **CVE ID : CVE-2021-38497**	g/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://www.mozilla.org/security/advisories/mfsa2021-47/, https://bugzilla.mozilla.org/show_bug.cgi?id=1726621	181121/353
Use After Free	03-Nov-21	5	During process shutdown, a document could have caused a use-after-free of a languages service object, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2. **CVE ID : CVE-2021-38498**	https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://bugzilla.mozilla.org/show_bug.cgi?id=1729642, https://www.mozilla.org/security/advisories/mfsa2021-47/	A-MOZ-FIRE-181121/354
N/A	03-Nov-21	6.8	Mozilla developers reported memory safety bugs	https://www.mozilla.or	A-MOZ-FIRE-181121/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			present in Firefox 92. 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 < 93. **CVE ID : CVE-2021-38499**	g/security/advisories/mfsa2021-43/	
N/A	03-Nov-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. 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 Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR < 91.2, Firefox ESR < 78.15, and Firefox < 93. **CVE ID : CVE-2021-38500**	https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://www.mozilla.org/security/advisories/mfsa2021-44/, https://www.mozilla.org/security/advisories/mfsa2021-47/	A-MOZ-FIRE-181121/356
N/A	03-Nov-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have	https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mf	A-MOZ-FIRE-181121/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			been exploited to run arbitrary code. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2. **CVE ID : CVE-2021-38501**	sa2021-45/, https://www.mozilla.org/security/advisories/mfsa2021-47/	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	03-Nov-21	5.8	Firefox incorrectly accepted a newline in a HTTP/3 header, interpretting it as two separate headers. This allowed for a header splitting attack against servers using HTTP/3. This vulnerability affects Firefox < 91.0.1 and Thunderbird < 91.0.1. **CVE ID : CVE-2021-29991**	https://www.mozilla.org/security/advisories/mfsa2021-37/	A-MOZ-FIRE-181121/358
N/A	03-Nov-21	5.8	Firefox for Android allowed navigations through the `intent://` protocol, which could be used to cause crashes and UI spoofs. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 92. **CVE ID : CVE-2021-29993**	https://www.mozilla.org/security/advisories/mfsa2021-38/	A-MOZ-FIRE-181121/359
firefox_esr					
N/A	03-Nov-21	4.3	When delegating navigations to the operating system, Firefox would accept the `mk` scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. *This bug only affects Firefox for Windows. Other operating	https://www.mozilla.org/security/advisories/mfsa2021-41/, https://www.mozilla.org/security/advisories/mfsa2021-40/,	A-MOZ-FIRE-181121/360

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
			systems are unaffected.*. This vulnerability affects Firefox < 92, Thunderbird < 91.1, Thunderbird < 78.14, Firefox ESR < 78.14, and Firefox ESR < 91.1. **CVE ID : CVE-2021-38492**	https://www.mozilla.org/security/advisories/mfsa2021-42/, https://www.mozilla.org/security/advisories/mfsa2021-38/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Nov-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 91 and Firefox ESR 78.13. 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 ESR < 78.14, Thunderbird < 78.14, and Firefox < 92. **CVE ID : CVE-2021-38493**	https://www.mozilla.org/security/advisories/mfsa2021-42/, https://www.mozilla.org/security/advisories/mfsa2021-38/, https://www.mozilla.org/security/advisories/mfsa2021-39/, https://bugzilla.mozilla.org/buglist.cgi?bug_id=1723391%2C1724101%2C1724107	A-MOZ-FIRE-181121/361
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Nov-21	6.8	Mozilla developers reported memory safety bugs present in Thunderbird 78.13.0. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could	https://www.mozilla.org/security/advisories/mfsa2021-41/, https://www.mozilla.org/security/a	A-MOZ-FIRE-181121/362

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
			have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 91.1 and Firefox ESR < 91.1. **CVE ID : CVE-2021-38495**	dvisories/mfsa2021-40/	
Use After Free	03-Nov-21	6.8	During operations on MessageTasks, a task may have been removed while it was still scheduled, resulting in memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR < 91.2, Firefox ESR < 78.15, and Firefox < 93. **CVE ID : CVE-2021-38496**	https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://www.mozilla.org/security/advisories/mfsa2021-44/, https://www.mozilla.org/security/advisories/mfsa2021-47/	A-MOZ-FIRE-181121/363
Origin Validation Error	03-Nov-21	4.3	Through use of reportValidity() and window.open(), a plain-text validation message could have been overlaid on another origin, leading to possible user confusion and spoofing attacks. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2. **CVE ID : CVE-2021-38497**	https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://www.mozilla.org/security/advisories/mf	A-MOZ-FIRE-181121/364

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
				sa2021-47/, https://bugzilla.mozilla.org/show_bug.cgi?id=1726621	
Use After Free	03-Nov-21	5	During process shutdown, a document could have caused a use-after-free of a languages service object, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2. **CVE ID : CVE-2021-38498**	https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://bugzilla.mozilla.org/show_bug.cgi?id=1729642, https://www.mozilla.org/security/advisories/mfsa2021-47/	A-MOZ-FIRE-181121/365
N/A	03-Nov-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. 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 Thunderbird < 78.15, Thunderbird < 91.2, Firefox	https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://www.mozilla.org/security/advisories/mf	A-MOZ-FIRE-181121/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ESR < 91.2, Firefox ESR < 78.15, and Firefox < 93. **CVE ID : CVE-2021-38500**	sa2021-44/, https://www.mozilla.org/security/advisories/mfsa2021-47/	
N/A	03-Nov-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. 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 < 93, Thunderbird < 91.2, and Firefox ESR < 91.2. **CVE ID : CVE-2021-38501**	https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://www.mozilla.org/security/advisories/mfsa2021-47/	A-MOZ-FIRE-181121/367
thunderbird					
N/A	03-Nov-21	4.3	When delegating navigations to the operating system, Firefox would accept the `mk` scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. *This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 92, Thunderbird < 91.1, Thunderbird < 78.14, Firefox ESR < 78.14, and Firefox ESR < 91.1. **CVE ID : CVE-2021-38492**	https://www.mozilla.org/security/advisories/mfsa2021-41/, https://www.mozilla.org/security/advisories/mfsa2021-40/, https://www.mozilla.org/security/advisories/mfsa2021-42/, https://www.mozilla.org/security/a	A-MOZ-THUN-181121/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				dvisories/mfsa2021-38/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Nov-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 91 and Firefox ESR 78.13. 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 ESR < 78.14, Thunderbird < 78.14, and Firefox < 92. **CVE ID : CVE-2021-38493**	https://www.mozilla.org/security/advisories/mfsa2021-42/, https://www.mozilla.org/security/advisories/mfsa2021-38/, https://www.mozilla.org/security/advisories/mfsa2021-39/, https://bugzilla.mozilla.org/buglist.cgi?bug_id=1723391%2C1724101%2C1724107	A-MOZ-THUN-181121/369
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Nov-21	6.8	Mozilla developers reported memory safety bugs present in Thunderbird 78.13.0. 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 Thunderbird < 91.1 and Firefox ESR < 91.1. **CVE ID : CVE-2021-38495**	https://www.mozilla.org/security/advisories/mfsa2021-41/, https://www.mozilla.org/security/advisories/mfsa2021-40/	A-MOZ-THUN-181121/370
Use After	03-Nov-21	6.8	During operations on MessageTasks, a task may	https://www.mozilla.or	A-MOZ-THUN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			have been removed while it was still scheduled, resulting in memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR < 91.2, Firefox ESR < 78.15, and Firefox < 93. **CVE ID : CVE-2021-38496**	g/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://www.mozilla.org/security/advisories/mfsa2021-44/, https://www.mozilla.org/security/advisories/mfsa2021-47/	181121/371
Origin Validation Error	03-Nov-21	4.3	Through use of reportValidity() and window.open(), a plain-text validation message could have been overlaid on another origin, leading to possible user confusion and spoofing attacks. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2. **CVE ID : CVE-2021-38497**	https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://www.mozilla.org/security/advisories/mfsa2021-47/, https://bugzilla.mozilla.org/show_bug.cgi?id=1726621	A-MOZ-THUN-181121/372
Use After Free	03-Nov-21	5	During process shutdown, a document could have	https://www.mozilla.or	A-MOZ-THUN-181121/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			caused a use-after-free of a languages service object, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2. **CVE ID : CVE-2021-38498**	g/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://bugzilla.mozilla.org/show_bug.cgi?id=1729642, https://www.mozilla.org/security/advisories/mfsa2021-47/	
N/A	03-Nov-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. 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 Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR < 91.2, Firefox ESR < 78.15, and Firefox < 93. **CVE ID : CVE-2021-38500**	https://www.mozilla.org/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://www.mozilla.org/security/advisories/mfsa2021-44/, https://www.mozilla.org/security/advisories/mfsa2021-47/	A-MOZ-THUN-181121/374
N/A	03-Nov-21	6.8	Mozilla developers reported memory safety bugs	https://www.mozilla.or	A-MOZ-THUN-181121/375

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
			present in Firefox 92 and Firefox ESR 91.1. 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 < 93, Thunderbird < 91.2, and Firefox ESR < 91.2. **CVE ID : CVE-2021-38501**	g/security/advisories/mfsa2021-43/, https://www.mozilla.org/security/advisories/mfsa2021-45/, https://www.mozilla.org/security/advisories/mfsa2021-47/	
Insufficiently Protected Credentials	03-Nov-21	4.3	Thunderbird ignored the configuration to require STARTTLS security for an SMTP connection. A MITM could perform a downgrade attack to intercept transmitted messages, or could take control of the authenticated session to execute SMTP commands chosen by the MITM. If an unprotected authentication method was configured, the MITM could obtain the authentication credentials, too. This vulnerability affects Thunderbird < 91.2. **CVE ID : CVE-2021-38502**	https://bugzilla.mozilla.org/show_bug.cgi?id=1733366, https://www.mozilla.org/security/advisories/mfsa2021-47/	A-MOZ-THUN-181121/376
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	03-Nov-21	5.8	Firefox incorrectly accepted a newline in a HTTP/3 header, interpretting it as two separate headers. This allowed for a header splitting attack against servers using HTTP/3. This vulnerability affects Firefox < 91.0.1 and Thunderbird <	https://www.mozilla.org/security/advisories/mfsa2021-37/	A-MOZ-THUN-181121/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			91.0.1. **CVE ID : CVE-2021-29991**		
Mybb					
mybb					
Improper Control of Generation of Code ('Code Injection')	04-Nov-21	6.5	MyBB before 1.8.29 allows Remote Code Injection by an admin with the "Can manage settings?" permission. The Admin CP's Settings management module does not validate setting types correctly on insertion and update, making it possible to add settings of supported type "php" with PHP code, executed on Change Settings pages. **CVE ID : CVE-2021-43281**	https://github.com/mybb/mybb/security/advisories/GHSA-8gxx-vmr9-h39p	A-MYB-MYBB-181121/378
navercorp					
whale					
N/A	02-Nov-21	5	Whale browser for iOS before 1.14.0 has an inconsistent user interface issue that allows an attacker to obfuscate the address bar which may lead to address bar spoofing. **CVE ID : CVE-2021-33593**	https://cve.naver.com/detail/cve-2021-43059	A-NAV-WHAL-181121/379
NEC					
clusterpro_x					
Buffer Copy without Checking Size of Input ('Classic Buffer	03-Nov-21	7.5	Buffer overflow vulnerability in the Disk Agent CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-CLUS-181121/380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			attacker to remote code execution via a network. **CVE ID : CVE-2021-20700**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Nov-21	7.5	Buffer overflow vulnerability in the Disk Agent CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote code execution via a network. **CVE ID : CVE-2021-20701**	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-CLUS-181121/381
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Nov-21	7.5	Buffer overflow vulnerability in the Transaction Server CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote code execution via a network. **CVE ID : CVE-2021-20702**	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-CLUS-181121/382
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Nov-21	7.5	Buffer overflow vulnerability in the Transaction Server CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote code execution via a network. **CVE ID : CVE-2021-20703**	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-CLUS-181121/383
Buffer Copy without Checking Size of Input ('Classic Buffer	03-Nov-21	7.5	Buffer overflow vulnerability in the compatible API with previous versions CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-CLUS-181121/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Windows and later allows attacker to remote code execution via a network. **CVE ID : CVE-2021-20704**		
Improper Input Validation	03-Nov-21	5	Improper input validation vulnerability in the WebManager CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote file upload via network. **CVE ID : CVE-2021-20705**	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-CLUS-181121/385
Improper Input Validation	03-Nov-21	5	Improper input validation vulnerability in the WebManager CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote file upload via network. **CVE ID : CVE-2021-20706**	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-CLUS-181121/386
Improper Input Validation	03-Nov-21	5	Improper input validation vulnerability in the Transaction Server CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to read files upload via network.. **CVE ID : CVE-2021-20707**	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-CLUS-181121/387
expresscluster_x					
Buffer Copy without Checking Size of Input ('Classic	03-Nov-21	7.5	Buffer overflow vulnerability in the Disk Agent CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for	https://jpn.nec.com/security-info/secinfo/nv21-	A-NEC-EXPR-181121/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Windows and later allows attacker to remote code execution via a network. **CVE ID : CVE-2021-20700**	015_en.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Nov-21	7.5	Buffer overflow vulnerability in the Disk Agent CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote code execution via a network. **CVE ID : CVE-2021-20701**	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-EXPR-181121/389
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Nov-21	7.5	Buffer overflow vulnerability in the Transaction Server CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote code execution via a network. **CVE ID : CVE-2021-20702**	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-EXPR-181121/390
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Nov-21	7.5	Buffer overflow vulnerability in the Transaction Server CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote code execution via a network. **CVE ID : CVE-2021-20703**	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-EXPR-181121/391
Buffer Copy without Checking Size of Input ('Classic Buffer	03-Nov-21	7.5	Buffer overflow vulnerability in the compatible API with previous versions CLUSTERPRO X 1.0 for Windows and later,	https://jpn.nec.com/security-info/secinfo/nv21-	A-NEC-EXPR-181121/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote code execution via a network. **CVE ID : CVE-2021-20704**	015_en.html	
Improper Input Validation	03-Nov-21	5	Improper input validation vulnerability in the WebManager CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote file upload via network. **CVE ID : CVE-2021-20705**	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-EXPR-181121/393
Improper Input Validation	03-Nov-21	5	Improper input validation vulnerability in the WebManager CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote file upload via network. **CVE ID : CVE-2021-20706**	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-EXPR-181121/394
Improper Input Validation	03-Nov-21	5	Improper input validation vulnerability in the Transaction Server CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to read files upload via network.. **CVE ID : CVE-2021-20707**	https://jpn.nec.com/security-info/secinfo/nv21-015_en.html	A-NEC-EXPR-181121/395
neoan					
neoan3-template					
Incorrect Permission Assignment	08-Nov-21	7.5	### Impact Versions prior 1.1.1 have allowed for passing in closures directly	https://github.com/sroehrl/neoan3-	A-NEO-NEOA-181121/396

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
for Critical Resource			into the template engine. As a result values that are callable are executed by the template engine. The issue arises if a value has the same name as a method or function in scope and can therefore be executed either by mistake or maliciously. In theory all users of the package are affected as long as they either deal with direct user input or database values. A multi-step attack on is therefore plausible. ### Patches Version 1.1.1 has addressed this vulnerability. ```php $params = ['reverse' => fn($input) => strrev($input), // <-- no longer possible with version ~1.1.1 'value' => 'My website'] TemplateFunctions::registerClosure('reverse', fn($input) => strrev($input)); // <-- still possible (and nicely isolated) Template::embrace('<h1>{{ reverse(value)}}</h1>', $params); ``` ### Workarounds Unfortunately only working with hardcoded values is safe in prior versions. As this likely defeats the purpose of a template engine, please upgrade. ###	template/security/advisories/GHSA-3v56-q6r6-4gcw, https://github.com/sroehrl/neoan3-template/issues/8, https://github.com/sroehrl/neoan3-template/commit/4a2c9570f071d3c8f4ac790007599cba20e16934	

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
			References As a possible exploit is relatively easy to achieve, I will not share steps to reproduce the issue for now. ### For more information If you have any questions or comments about this advisory: * Open an issue in [our repo](https://github.com/sroehrl/neoan3-template) **CVE ID : CVE-2021-41170**		
Netapp					
ontap_system_manager					
Insecure Storage of Sensitive Information	01-Nov-21	1.7	System Manager 9.x versions 9.7 and higher prior to 9.7P16, 9.8P7 and 9.9.1P2 are susceptible to a vulnerability which could allow a local attacker to discover plaintext iSCSI CHAP credentials. **CVE ID : CVE-2021-27004**	https://security.netapp.com/advisory/NTAP-20211029-0001/	A-NET-ONTA-181121/397
Uncontrolled Resource Consumption	01-Nov-21	5	Clustered Data ONTAP versions 9.6 and higher prior to 9.6P16, 9.7P16, 9.8P7 and 9.9.1P3 are susceptible to a vulnerability which could allow a remote attacker to cause a crash of the httpd server. **CVE ID : CVE-2021-27005**	https://security.netapp.com/advisory/NTAP-20211029-0002/	A-NET-ONTA-181121/398
nextscripts					
social_networks_auto_poster					
Improper Neutralization of Input	01-Nov-21	4.3	The NextScripts: Social Networks Auto-Poster <= 4.3.20 WordPress plugin is	N/A	A-NEX-SOCI-181121/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerable to Reflected Cross-Site Scripting via the $_REQUEST['page'] parameter which is echoed out on inc/nxs_class_snap.php by supplying the appropriate value 'nxssnap-post' to load the page in $_GET['page'] along with malicious JavaScript in $_POST['page']. **CVE ID : CVE-2021-38356**		
Nlnetlabs					
routinator					
Uncontrolled Recursion	09-Nov-21	5	NLnet Labs Routinator prior to 0.10.2 happily processes a chain of RRDP repositories of infinite length causing it to never finish a validation run. In RPKI, a CA can choose the RRDP repository it wishes to publish its data in. By continuously generating a new child CA that only consists of another CA using a different RRDP repository, a malicious CA can create a chain of CAs of de-facto infinite length. Routinator prior to version 0.10.2 did not contain a limit on the length of such a chain and will therefore continue to process this chain forever. As a result, the validation run will never finish, leading to Routinator continuing to serve the old	https://www.nlnetlabs.nl/downloads/routinator/CVE-2021-43172_CVE-2021-43173_CVE-2021-43174.txt	A-NLN-ROUT-181121/400

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
			data set or, if in the initial validation run directly after starting, never serve any data at all. **CVE ID : CVE-2021-43172**		
Improper Handling of Exceptional Conditions	09-Nov-21	5	In NLnet Labs Routinator prior to 0.10.2, a validation run can be delayed significantly by an RRDP repository by not answering but slowly drip-feeding bytes to keep the connection alive. This can be used to effectively stall validation. While Routinator has a configurable time-out value for RRDP connections, this time-out was only applied to individual read or write operations rather than the complete request. Thus, if an RRDP repository sends a little bit of data before that time-out expired, it can continuously extend the time it takes for the request to finish. Since validation will only continue once the update of an RRDP repository has concluded, this delay will cause validation to stall, leading to Routinator continuing to serve the old data set or, if in the initial validation run directly after starting, never serve any data at all. **CVE ID : CVE-2021-43173**	https://www.nlnetlabs.nl/downloads/routinator/CVE-2021-43172_CVE-2021-43173_CVE-2021-43174.txt	A-NLN-ROUT-181121/401
Out-of-	09-Nov-21	5	NLnet Labs Routinator	https://ww	A-NLN-ROUT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			versions 0.9.0 up to and including 0.10.1, support the gzip transfer encoding when querying RRDP repositories. This encoding can be used by an RRDP repository to cause an out-of-memory crash in these versions of Routinator. RRDP uses XML which allows arbitrary amounts of white space in the encoded data. The gzip scheme compresses such white space extremely well, leading to very small compressed files that become huge when being decompressed for further processing, big enough that Routinator runs out of memory when parsing input data waiting for the next XML element. **CVE ID : CVE-2021-43174**	w.nlnetlabs.nl/downloads/routinator/CVE-2021-43172_CVE-2021-43173_CVE-2021-43174.txt	181121/402
nsasoft					
spotauditor					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Nov-21	5	An issue was discovered in Nsasoft US LLC SpotAuditor 5.3.5. The program can be crashed by entering 300 bytes char data into the "Key" or "Name" field while registering. **CVE ID : CVE-2021-27722**	N/A	A-NSA-SPOT-181121/403
obsidian					
obsidian_dataview					
Improper	04-Nov-21	9.3	Obsidian Dataview through	N/A	A-OBS-OBSI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control of Generation of Code ('Code Injection')			0.4.12-hotfix1 allows eval injection. The evalInContext function in executes user input, which allows an attacker to craft malicious Markdown files that will execute arbitrary code once opened. NOTE: 0.4.13 provides a mitigation for some use cases. **CVE ID : CVE-2021-42057**		181121/404
online_enrollment_management_system_in_php_project					
online_enrollment_management_system_in_php					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	3.5	A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Online Enrollment Management System in PHP and PayPal Free Source Code 1.0 in the Add-Users page via the Name parameter. **CVE ID : CVE-2021-40577**	N/A	A-ONL-ONLI-181121/405
online_event_booking_and_reservation_system_project					
online_event_booking_and_reservation_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-21	3.5	A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Online Event Booking and Reservation System in PHP/MySQL via the Holiday reason parameter. An attacker can leverage this vulnerability in order to run javascript commands on the web server surfers behalf, which can lead to cookie	N/A	A-ONL-ONLI-181121/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			stealing and more. **CVE ID : CVE-2021-42662**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Nov-21	4.3	An HTML injection vulnerability exists in Sourcecodester Online Event Booking and Reservation System in PHP/MySQL via the msg parameter to /event-management/index.php. An attacker can leverage this vulnerability in order to change the visibility of the website. Once the target user clicks on a given link he will display the content of the HTML code of the attacker's choice. **CVE ID : CVE-2021-42663**	N/A	A-ONL-ONLI-181121/407
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Nov-21	7.5	A SQL Injection vulnerability exists in Sourcecodester Online Event Booking and Reservation System in PHP in event-management/views. An attacker can leverage this vulnerability in order to manipulate the sql query performed. As a result he can extract sensitive data from the web server and in some cases he can use this vulnerability in order to get a remote code execution on the remote web server. **CVE ID : CVE-2021-42667**	N/A	A-ONL-ONLI-181121/408
opengamepanel					
opengamepanel					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	10-Nov-21	9	An issue was discovered in OpenGamePanel OGP-Agent-Linux through 2021-08-14. $HOME/OGP/Cfg/Config.pm has the root password in cleartext. **CVE ID : CVE-2021-37157**	https://github.com/OpenGamePanel/OGP-Agent-Linux/commits/master	A-OPE-OPEN-181121/409
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Nov-21	9	An issue was discovered in OpenGamePanel OGP-Agent-Linux through 2021-08-14. An authenticated attacker could inject OS commands by starting a Counter-Strike server and using the map field to enter a Bash command. **CVE ID : CVE-2021-37158**	N/A	A-OPE-OPEN-181121/410
opnsense					
opnsense					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	4.3	A Cross-site scripting (XSS) vulnerability was discovered in OPNsense before 21.7.4 via the LDAP attribute return in the authentication tester. **CVE ID : CVE-2021-42770**	https://opnsense.org/opnsense-21-7-4-released/	A-OPN-OPNS-181121/411
oppia					
oppia					
URL Redirection to Untrusted Site ('Open Redirect')	08-Nov-21	5.8	Oppia 3.1.4 does not verify that certain URLs are valid before navigating to them. **CVE ID : CVE-2021-41733**	https://github.com/oppia/oppia/pull/13892	A-OPP-OPPI-181121/412
optinmonster					
optinmonster					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	01-Nov-21	6.4	The OptinMonster WordPress plugin is vulnerable to sensitive information disclosure and unauthorized setting updates due to insufficient authorization validation via the logged_in_or_has_api_key function in the ~/OMAPI/RestApi.php file that can used to exploit inject malicious web scripts on sites with the plugin installed. This affects versions up to, and including, 2.6.4. **CVE ID : CVE-2021-39341**	N/A	A-OPT-OPTI-181121/413
Owasp					
owasp_modsecurity_core_rule_set					
Incorrect Authorization	05-Nov-21	7.5	OWASP ModSecurity Core Rule Set 3.1.x before 3.1.2, 3.2.x before 3.2.1, and 3.3.x before 3.3.2 is affected by a Request Body Bypass via a trailing pathname. **CVE ID : CVE-2021-35368**	https://portswigger.net/daily-swig/waf-bypass-severe-owasp-modsecurity-core-rule-set-bug-was-present-for-several-years, https://coreruleset.org/20210630/cve-2021-35368-crs-request-body-	A-OWA-OWAS-181121/414

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
				bypass/, https://owasp.org/www-project-modsecurity-core-rule-set/	
Phoenixcontact					
pc_worx					
Improper Input Validation	04-Nov-21	6.8	Improper Input Validation vulnerability in PC Worx Automation Suite of Phoenix Contact up to version 1.88 could allow an attacker with a manipulated project file to unpack arbitrary files outside of the selected project directory. **CVE ID : CVE-2021-34597**	https://cert.vde.com/en/advisories/VDE-2021-052/	A-PHO-PC_W-181121/415
pc_worx_express					
Improper Input Validation	04-Nov-21	6.8	Improper Input Validation vulnerability in PC Worx Automation Suite of Phoenix Contact up to version 1.88 could allow an attacker with a manipulated project file to unpack arbitrary files outside of the selected project directory. **CVE ID : CVE-2021-34597**	https://cert.vde.com/en/advisories/VDE-2021-052/	A-PHO-PC_W-181121/416
phoenix_media_rename_project					
phoenix_media_rename					
N/A	08-Nov-21	4	The Phoenix Media Rename WordPress plugin before 3.4.4 does not have capability checks in its phoenix_media_rename AJAX action, which could	N/A	A-PHO-PHOE-181121/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow users with Author roles to rename any uploaded media files, including ones they do not own. **CVE ID : CVE-2021-24816**		
phone_shop_sales_management_system_project					
phone_shop_sales_management_system					
Improper Authentication	02-Nov-21	7.5	Phone Shop Sales Managements System using PHP with Source Code 1.0 is vulnerable to authentication bypass which leads to account takeover of the admin. **CVE ID : CVE-2021-36560**	N/A	A-PHO-PHON-181121/418
php_event_calendar_project					
php_event_calendar					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	4.3	PHP Event Calendar through 2021-11-04 allows persistent cross-site scripting (XSS), as demonstrated by the /server/ajax/events_manager.php title parameter. This can be exploited by an adversary in multiple ways, e.g., to perform actions on the page in the context of other users, or to deface the site. **CVE ID : CVE-2021-42078**	N/A	A-PHP-PHP_-181121/419
playtuber_project					
playtuber					
N/A	03-Nov-21	6.5	An issue was discoverered in in customercentric-selling-poland PlayTube,	N/A	A-PLA-PLAY-181121/420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows authenticated attackers to execute arbitrary code via the purchace code to the config.php. **CVE ID : CVE-2021-26786**		
pomerium					
pomerium					
Incorrect Authorization	05-Nov-21	6.5	Pomerium is an open source identity-aware access proxy. In affected versions changes to the OIDC claims of a user after initial login are not reflected in policy evaluation when using `allowed_idp_claims` as part of policy. If using `allowed_idp_claims` and a user's claims are changed, Pomerium can make incorrect authorization decisions. This issue has been resolved in v0.15.6. For users unable to upgrade clear data on `databroker` service by clearing redis or restarting the in-memory databroker to force claims to be updated. **CVE ID : CVE-2021-41230**	https://github.com/pomerium/pomerium/security/advisories/GHSA-j6wp-3859-vxfg, https://github.com/pomerium/pomerium/pull/2724	A-POM-POME-181121/421
post_content_xmlrpc_project					
post_content_xmlrpc					
Improper Neutralization of Special Elements used in an	08-Nov-21	6.5	The Post Content XMLRPC WordPress plugin through 1.0 does not sanitise or escape multiple GET/POST parameters before using	N/A	A-POS-POST-181121/422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			them in SQL statements in the admin dashboard, leading to an authenticated SQL Injections **CVE ID : CVE-2021-24629**		
poweradmin					
pa_server_monitor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-21	3.5	A cross-site scripting (XSS) vulnerability in Power Admin PA Server Monitor 8.2.1.1 allows remote attackers to inject arbitrary web script or HTML via Console.exe. **CVE ID : CVE-2021-26844**	https://www.poweradmin.com/products/server-monitoring/support/release-notes/	A-POW-PA_S-181121/423
print-o-matic_project					
print-o-matic					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	3.5	The Print-O-Matic WordPress plugin before 2.0.3 does not escape some of its settings before outputting them in attribute, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24710**	https://plugins.trac.wordpress.org/changeset/2610060/	A-PRI-PRIN-181121/424
publify_project					
publify					
Incorrect Authorization	02-Nov-21	6.5	In Publify, 9.0.0.pre1 to 9.2.4 are vulnerable to Improper Access Control. “guest” role users can self-register even when the admin does not allow. This	https://github.com/publify/publify/commit/3447e0241e921b65f6eb1090	A-PUB-PUBL-181121/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			happens due to front-end restriction only. **CVE ID : CVE-2021-25973**	453d8ea73e98387e	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-21	3.5	In Publify, versions v8.0 to v9.2.4 are vulnerable to stored XSS. A user with a “publisher” role is able to inject and execute arbitrary JavaScript code while creating a page/article. **CVE ID : CVE-2021-25974**	https://github.com/publify/publify/commit/fefd5f76302adcc425b2b6e7ed23587cfc0083e	A-PUB-PUBL-181121/426
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-21	3.5	In publify, versions v8.0 to v9.2.4 are vulnerable to stored XSS as a result of an unrestricted file upload. This issue allows a user with “publisher” role to inject malicious JavaScript via the uploaded html file. **CVE ID : CVE-2021-25975**	https://github.com/publify/publify/commit/d99c0870d3dbbfde7febdc6cad33199b84770101	A-PUB-PUBL-181121/427
publishpress					
post_expirator					
Incorrect Authorization	08-Nov-21	4	The Post Expirator WordPress plugin before 2.6.0 does not have proper capability checks in place, which could allow users with a role as low as Contributor to schedule deletion of arbitrary posts. **CVE ID : CVE-2021-24783**	N/A	A-PUB-POST-181121/428
quiz_tool_lite_project					
quiz_tool_lite					
Improper Neutralization of Input During Web	08-Nov-21	3.5	The Quiz Tool Lite WordPress plugin through 2.3.15 does not sanitize multiple input fields used	N/A	A-QUI-QUIZ-181121/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			when creating or managing quizzes and in other setting options, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24701**		
qwizcards_project					
qwizcards					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	3.5	The Qwizcards â€“ online quizzes and flashcards WordPress plugin before 3.62 does not properly sanitize and escape 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-2021-24706**	N/A	A-QWI-QWIZ-181121/430
radiustheme					
logo_slider_and_showcase					
Incorrect Authorization	01-Nov-21	4	The Logo Slider and Showcase WordPress plugin before 1.3.37 allows Editor users to update the plugin's settings via the rtWLSSettings AJAX action because it uses a nonce for authorisation instead of a capability check. **CVE ID : CVE-2021-24742**	N/A	A-RAD-LOGO-181121/431
Realtek					
rtsupx_usb_utility_driver					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	02-Nov-21	7.2	RtsUpx.sys in Realtek RtsUpx USB Utility Driver for Camera/Hub/Audio through 1.14.0.0 allows local low-privileged users to achieve unauthorized access to USB devices (Escalation of Privileges, Denial of Service, Code Execution, and Information Disclosure) via a crafted Device IO Control packet to a device. **CVE ID : CVE-2021-36922**	https://www.realtek.com/images/safe-report/Realtek_RtsUpx_Security_Advisory_Report.pdf	A-REA-RTSU-181121/432
Improper Privilege Management	02-Nov-21	7.2	RtsUpx.sys in Realtek RtsUpx USB Utility Driver for Camera/Hub/Audio through 1.14.0.0 allows local low-privileged users to achieve unauthorized access to USB device privileged IN and OUT instructions (leading to Escalation of Privileges, Denial of Service, Code Execution, and Information Disclosure) via a crafted Device IO Control packet to a device. **CVE ID : CVE-2021-36923**	https://www.realtek.com/images/safe-report/Realtek_RtsUpx_Security_Advisory_Report.pdf	A-REA-RTSU-181121/433
Uncontrolled Resource Consumption	02-Nov-21	7.2	RtsUpx.sys in Realtek RtsUpx USB Utility Driver for Camera/Hub/Audio through 1.14.0.0 allows local low-privileged users to achieve a pool overflow (leading to Escalation of Privileges, Denial of Service, and Code Execution) via a crafted Device IO Control	https://www.realtek.com/images/safe-report/Realtek_RtsUpx_Security_Advisory_Report.pdf	A-REA-RTSU-181121/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packet to a device. **CVE ID : CVE-2021-36924**		
N/A	02-Nov-21	7.2	RtsUpx.sys in Realtek RtsUpx USB Utility Driver for Camera/Hub/Audio through 1.14.0.0 allows local low-privileged users to achieve an arbitrary read or write operation from/to physical memory (leading to Escalation of Privileges, Denial of Service, Code Execution, and Information Disclosure) via a crafted Device IO Control packet to a device. **CVE ID : CVE-2021-36925**	https://www.realtek.com/images/safe-report/Realtek_RtsUpx_Security_Advisory_Report.pdf	A-REA-RTSU-181121/435
remoteclinic					
remote_clinic					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-21	4.3	Multiple Cross Site Scripting (XSS) vulnerabilities exists in Remote Clinic v2.0 in (1) patients/register-patient.php via the (a) Contact, (b) Email, (c) Weight, (d) Profession, (e) ref_contact, (f) address, (g) gender, (h) age, and (i) serial parameters; in (2) patients/edit-patient.php via the (a) Contact, (b) Email, (c) Weight, Profession, (d) ref_contact, (e) address, (f) serial, (g) age, and (h) gender parameters; in (3) staff/edit-my-profile.php via the (a) Title, (b) First Name, (c) Last Name, (d)	https://remoteclinic.io	A-REM-REMO-181121/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Skype, and (e) Address parameters; and in (4) clinics/settings.php via the (a) portal_name, (b) guardian_short_name, (c) guardian_name, (d) opening_time, (e) closing_time, (f) access_level_5, (g) access_level_4, (h) access_level_ 3, (i) access_level_2, (j) access_level_1, (k) currency, (l) mobile_number, (m) address, (n) patient_contact, (o) patient_address, and (p) patient_email parameters. **CVE ID : CVE-2021-39416**		
replicated					
replicated_classic					
URL Redirection to Untrusted Site ('Open Redirect')	01-Nov-21	5.8	An open redirect vulnerability exists in Replicated Classic versions prior to 2.53.1 that could lead to spoofing. To exploit this vulnerability, an attacker could send a link that has a specially crafted URL and convince the user to click the link, redirecting the user to an untrusted site. **CVE ID : CVE-2021-43058**	https://www.replicated.com/security/advisories/CVE-2021-43058	A-REP-REPL-181121/437
s-cart					
s-cart					
Unrestricted Upload of File with	01-Nov-21	6.5	S-Cart v6.4.1 and below was discovered to contain an arbitrary file upload	N/A	A-S-C-S-CA-181121/438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			vulnerability in the Editor module on the Admin panel. This vulnerability allows attackers to execute arbitrary code via a crafted IMG file. **CVE ID : CVE-2021-38847**		
Samsung					
group_sharing					
Improper Input Validation	05-Nov-21	2.1	Intent redirection vulnerability in Group Sharing prior to 10.8.03.2 allows attacker to access contact information. **CVE ID : CVE-2021-25504**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=11	A-SAM-GROU-181121/439
health					
Incorrect Authorization	05-Nov-21	2.1	Non-existent provider in Samsung Health prior to 6.19.1.0001 allows attacker to access it via malicious content provider or lead to denial of service. **CVE ID : CVE-2021-25506**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=11	A-SAM-HEAL-181121/440
samsung_flow					
Incorrect Authorization	05-Nov-21	2.7	Improper authorization vulnerability in Samsung Flow mobile application prior to 4.8.03.5 allows Samsung Flow PC application connected with user device to access part of notification data in Secure Folder without authorization. **CVE ID : CVE-2021-25507**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=11	A-SAM-SAMS-181121/441
Improper	05-Nov-21	3.6	A missing input validation	https://secu	A-SAM-SAMS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			in Samsung Flow Windows application prior to Version 4.8.5.0 allows attackers to overwrite abtraty file in the Windows known folders. **CVE ID : CVE-2021-25509**	rity.samsungmobile.com/serviceWeb.smsb?year=2021&month=11	181121/442
samsung_pass					
Improper Authentication	05-Nov-21	6.8	Improper authentication in Samsung Pass prior to 3.0.02.4 allows to use app without authentication when lockscreen is unlocked. **CVE ID : CVE-2021-25505**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=11	A-SAM-SAMS-181121/443
smartthings					
Improper Privilege Management	05-Nov-21	7.5	Improper privilege management vulnerability in API Key used in SmartThings prior to 1.7.73.22 allows an attacker to abuse the API key without limitation. **CVE ID : CVE-2021-25508**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=11	A-SAM-SMAR-181121/444
SAP					
abap_platform_kernel					
Missing Authorization	10-Nov-21	5.5	SAP ABAP Platform Kernel - versions 7.77, 7.81, 7.85, 7.86, does not perform necessary authorization checks for an authenticated business user, resulting in escalation of privileges. That means this business user is able to read and modify data beyond the vulnerable system. However, the attacker can neither significantly reduce	https://launchpad.support.sap.com/#/notes/3099776, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=589496864	A-SAP-ABAP-181121/445

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 performance of the system nor stop the system. **CVE ID : CVE-2021-40501**		
commerce					
Missing Authorization	10-Nov-21	6.5	SAP Commerce - versions 2105.3, 2011.13, 2005.18, 1905.34, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. Authenticated attackers will be able to access and edit data from B2B units they do not belong to. **CVE ID : CVE-2021-40502**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=589496864 , https://launchpad.support.sap.com/#/notes/3110328	A-SAP-COMM-181121/446
netweaver_application_server_for_abap					
Incorrect Authorization	10-Nov-21	4	A certain template role in SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, contains transport authorizations, which exceed expected display only permissions. **CVE ID : CVE-2021-40504**	https://launchpad.support.sap.com/#/notes/3105728, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=589496864	A-SAP-NETW-181121/447
schiocco					
support_board					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	3.5	The Support Board WordPress plugin before 3.3.5 allows Authenticated (Agent+) users to perform Cross-Site Scripting attacks by placing a payload in the notes field, when an administrator or any	N/A	A-SCH-SUPP-181121/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user go to the chat the XSS will be automatically executed. **CVE ID : CVE-2021-24807**		
schreikasten_project					
schreikasten					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	6.5	The Schreikasten WordPress plugin through 0.14.18 does not sanitise or escape the id GET parameter before using it in SQL statements in the comments dashboard from various actions, leading to authenticated SQL Injections which can be exploited by users as low as author **CVE ID : CVE-2021-24630**	N/A	A-SCH-SCHR-181121/449
Seopanel					
seo_panel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-21	4.3	Multiple Cross Site Scripting (XSS) vulnerabilities exits in SEO Panel v4.8.0 via the (1) to_time parameter in (a) backlinks.php, (b) analytics.php, (c) log.php, (d) overview.php, (e) pagespeed.php, (f) rank.php, (g) review.php, (h) saturationchecker.php, (i) social_media.php, and (j) reports.php; the (2) from_time parameter in (a) backlinks.php, (b) analytics.php, (c) log.php, (d) overview.php, (e) pagespeed.php, (f)	N/A	A-SEO-SEO_-181121/450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			rank.php, (g) review.php, (h) saturationchecker.php, (i) social_media.php, (j) webmaster-tools.php, and (k) reports.php; the (3) order_col parameter in (a) analytics.php, (b) review.php, (c) social_media.php, and (d) webmaster-tools.php; and the (4) pageno parameter in (a) alerts.php, (b) log.php, (c) keywords.php, (d) proxy.php, (e) searchengine.php, and (f) siteauditor.php. **CVE ID : CVE-2021-39413**		
servicetonic					
servicetonic					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	5	Blind SQL injection in the login form in ServiceTonic Helpdesk software < 9.0.35937 allows attacker to exfiltrate information via specially crafted HQL-compatible time-based SQL queries. **CVE ID : CVE-2021-28022**	N/A	A-SER-SERV-181121/451
Unrestricted Upload of File with Dangerous Type	08-Nov-21	7.5	Arbitrary file upload in Service import feature in ServiceTonic Helpdesk software version < 9.0.35937 allows a malicious user to execute JSP code by uploading a zip that extracts files in relative paths. **CVE ID : CVE-2021-28023**	N/A	A-SER-SERV-181121/452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Nov-21	7.5	Unauthorized system access in the login form in ServiceTonic Helpdesk software version < 9.0.35937 allows attacker to login without using a password. **CVE ID : CVE-2021-28024**	N/A	A-SER-SERV-181121/453
Shareaholic					
similar_posts					
Improper Control of Generation of Code ('Code Injection')	08-Nov-21	6	The Similar Posts WordPress plugin through 3.1.5 allow high privilege users to execute arbitrary PHP code in an hardened environment (ie with DISALLOW_FILE_EDIT, DISALLOW_FILE_MODS and DISALLOW_UNFILTERED_HTML set to true) via the 'widget_rrm_similar_posts_condition' widget setting of the plugin. **CVE ID : CVE-2021-24537**	N/A	A-SHA-SIMI-181121/454
shopping_portal_project					
shopping_portal					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-21	4.3	Multiple Cross Site Scripting (XSS) vulnerabilities exists in PHPGurukul Shopping v3.1 via the (1) callback parameter in (a) server_side/scripts/id_jsonp.php, (b) server_side/scripts/jsonp.php, and (c) scripts/objects_jsonp.php, the (2) value parameter in examples_support/editable	N/A	A-SHO-SHOP-181121/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			_ajax.php, and the (3) PHP_SELF parameter in captcha/index.php. **CVE ID : CVE-2021-39412**		
Siemens					
capital_vstar					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network.	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-CAPI-181121/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(FSMD-2021-0004) **CVE ID : CVE-2021-31344**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-CAPI-181121/457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0006) **CVE ID : CVE-2021-31345**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory.	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-CAPI-181121/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(FSMD-2021-0007) **CVE ID : CVE-2021-31346**		
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-CAPI-181121/459
Improper Restriction	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC	https://cert-portal.sieme	A-SIE-CAPI-181121/460

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
of Operations within the Bounds of a Memory Buffer			(PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**	ns.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Restriction of Operations within the	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-	A-SIE-CAPI-181121/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**	044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/prod	A-SIE-CAPI-181121/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**	uctcert/pdf/ssa-114589.pdf	
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/	A-SIE-CAPI-181121/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**	ssa-114589.pdf	
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-CAPI-181121/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "USER" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-CAPI-181121/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "PWD/XPWD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-CAPI-181121/466

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
			ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "MKD/XMKD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-CAPI-181121/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**		
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-CAPI-181121/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**		
nucleus_net					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/470

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
			Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**		
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/472

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
			conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/474
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC	https://cert-portal.siemens.com/productcert/pdf/	A-SIE-NUCL-181121/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**	ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-	A-SIE-NUCL-181121/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**	044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/prod	A-SIE-NUCL-181121/477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "USER" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**	uctcert/pdf/ssa-114589.pdf	
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/478

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
			Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "PWD/XPWD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “MKD/XMKD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**		
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**		
nucleus_readystart_v3					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			< V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**		
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013)	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31883		
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/489
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC	https://cert-portal.siemens.com/productcert/pdf/	A-SIE-NUCL-181121/490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "USER" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**	ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-	A-SIE-NUCL-181121/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "PWD/XPWD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**	portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/	A-SIE-NUCL-181121/492

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
			Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "MKD/XMKD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**	ssa-114589.pdf	
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**		
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**		
nucleus_readystart_v4					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			< V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**		
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			< V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**		
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**		
nucleus_source_code					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked.	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**		
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0011) **CVE ID : CVE-2021-31882**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/504
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC	https://cert-portal.sieme	A-SIE-NUCL-181121/505

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
			(PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**	ns.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Buffer Access with Incorrect	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All	https://cert-portal.siemens.com/prod	A-SIE-NUCL-181121/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Length Value			versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**	uctcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-	A-SIE-NUCL-181121/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "USER" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**	portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/	A-SIE-NUCL-181121/508

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
			Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “PWD/XPWD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**	ssa-114589.pdf	
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "MKD/XMKD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**		
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	A-SIE-NUCL-181121/511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**		
sentron_powermanager_3					
Incorrect Permission Assignment for Critical Resource	09-Nov-21	7.2	A vulnerability has been identified in SENTRON powermanager V3 (All versions). The affected application assigns improper access rights to a specific folder containing configuration files. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges. **CVE ID : CVE-2021-37207**	https://cert-portal.siemens.com/productcert/pdf/ssa-537983.pdf	A-SIE-SENT-181121/512
simatic_pcs_7					
Improper Limitation of a Pathname to a Restricted Directory	09-Nov-21	7.5	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions), SIMATIC PCS 7 V9.1 (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-840188.pdf	A-SIE-SIMA-181121/513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			SIMATIC WinCC V15 and earlier (All versions), SIMATIC WinCC V16 (All versions), SIMATIC WinCC V17 (All versions), SIMATIC WinCC V7.4 and earlier (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 5). Legitimate file operations of the affected systems do not properly neutralize special elements within the pathname. An attacker could then cause the pathname to resolve to a location outside of the restricted directory on the server and read, write or delete unexpected critical files. **CVE ID : CVE-2021-40358**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Nov-21	5	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions), SIMATIC PCS 7 V9.1 (All versions), SIMATIC WinCC V15 and earlier (All versions), SIMATIC WinCC V16 (All versions), SIMATIC WinCC V17 (All versions), SIMATIC WinCC V7.4 and earlier (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 5). When downloading files, the affected systems do not properly neutralize special	https://cert-portal.siemens.com/productcert/pdf/ssa-840188.pdf	A-SIE-SIMA-181121/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			elements within the pathname. An attacker could then cause the pathname to resolve to a location outside of the restricted directory on the server and read unexpected critical files. **CVE ID : CVE-2021-40359**		
Insertion of Sensitive Information into Log File	09-Nov-21	5	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions), SIMATIC PCS 7 V9.1 (All versions), SIMATIC WinCC V15 and earlier (All versions), SIMATIC WinCC V16 (All versions), SIMATIC WinCC V17 (All versions), SIMATIC WinCC V7.4 and earlier (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 5). The affected systems store sensitive information in log files. An attacker with access to the log files could publicly expose the information or reuse it to develop further attacks on the system. **CVE ID : CVE-2021-40364**	https://cert-portal.siemens.com/productcert/pdf/ssa-840188.pdf	A-SIE-SIMA-181121/515
simatic_wincc					
Improper Limitation of a Pathname to a Restricted Directory	09-Nov-21	7.5	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions), SIMATIC PCS 7 V9.1 (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-840188.pdf	A-SIE-SIMA-181121/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			SIMATIC WinCC V15 and earlier (All versions), SIMATIC WinCC V16 (All versions), SIMATIC WinCC V17 (All versions), SIMATIC WinCC V7.4 and earlier (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 5). Legitimate file operations of the affected systems do not properly neutralize special elements within the pathname. An attacker could then cause the pathname to resolve to a location outside of the restricted directory on the server and read, write or delete unexpected critical files. **CVE ID : CVE-2021-40358**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Nov-21	5	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions), SIMATIC PCS 7 V9.1 (All versions), SIMATIC WinCC V15 and earlier (All versions), SIMATIC WinCC V16 (All versions), SIMATIC WinCC V17 (All versions), SIMATIC WinCC V7.4 and earlier (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 5). When downloading files, the affected systems do not properly neutralize special	https://cert-portal.siemens.com/productcert/pdf/ssa-840188.pdf	A-SIE-SIMA-181121/517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			elements within the pathname. An attacker could then cause the pathname to resolve to a location outside of the restricted directory on the server and read unexpected critical files. **CVE ID : CVE-2021-40359**		
Insertion of Sensitive Information into Log File	09-Nov-21	5	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions), SIMATIC PCS 7 V9.1 (All versions), SIMATIC WinCC V15 and earlier (All versions), SIMATIC WinCC V16 (All versions), SIMATIC WinCC V17 (All versions), SIMATIC WinCC V7.4 and earlier (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 5). The affected systems store sensitive information in log files. An attacker with access to the log files could publicly expose the information or reuse it to develop further attacks on the system. **CVE ID : CVE-2021-40364**	https://cert-portal.siemens.com/productcert/pdf/ssa-840188.pdf	A-SIE-SIMA-181121/518
simple_cashiering_system_project					
simple_cashiering_system					
Improper Neutralization of Special Elements used in an	03-Nov-21	7.5	Multiple SQL Injection vulnerabilities exist in Sourcecodester Simple Cashiering System (POS) 1.0 via the (1) Product Code in	N/A	A-SIM-SIMP-181121/519

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
SQL Command ('SQL Injection')			the pos page in cashiering. (2) id parameter in manage_products and the (3) t paramater in actions.php. **CVE ID : CVE-2021-41492**		
simple_subscription_website_project					
simple_subscription_website					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Nov-21	7.5	SQL Injection vulnerability exists in Sourcecodester. Simple Subscription Website 1.0. via the login. **CVE ID : CVE-2021-43140**	N/A	A-SIM-SIMP-181121/520
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-21	4.3	Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Simple Subscription Website 1.0 via the id parameter in plan_application. **CVE ID : CVE-2021-43141**	N/A	A-SIM-SIMP-181121/521
siren					
investigate					
N/A	02-Nov-21	6.8	In Siren Investigate before 11.1.4, when enabling the cluster feature of the Siren Alert application, TLS verifications are disabled globally in the Siren Investigate main process. **CVE ID : CVE-2021-36794**	https://docs.siren.io/siren-platform-user-guide/11.1/release-notes.html#_security_fixes_3, https://docs.siren.io/ind	A-SIR-INVE-181121/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ex, https://community.siren.io/c/announcements	
Sitecore					
experience_platform					
Deserialization of Untrusted Data	05-Nov-21	10	Sitecore XP 7.5 Initial Release to Sitecore XP 8.2 Update-7 is vulnerable to an insecure deserialization attack where it is possible to achieve remote command execution on the machine. No authentication or special configuration is required to exploit this vulnerability. **CVE ID : CVE-2021-42237**	http://sitecore.com, https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1000776	A-SIT-EXPE-181121/523
snowsoftware					
snow_inventory_agent					
N/A	03-Nov-21	3.6	A vulnerability in Snow Snow Agent for Windows allows a non-admin user to cause arbitrary deletion of files. This issue affects: Snow Snow Agent for Windows version 5.0.0 to 6.7.1 on Windows. **CVE ID : CVE-2021-41562**	https://community.snowsoftware.com/s/group/0F91r000000QUhPCAW/news-updates	A-SNO-SNOW-181121/524
sonaar					
mp3_audio_player_for_music\\,_radio_\\&_podcast					
Improper Neutralization of Input During Web Page	01-Nov-21	3.5	The MP3 Audio Player for Music, Radio & Podcast by Sonaar WordPress plugin before 2.4.2 does not properly sanitize or escape	N/A	A-SON-MP3_-181121/525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			data in some of its Playlist settings, allowing high privilege users to perform Cross-Site Scripting attacks **CVE ID : CVE-2021-24624**		
Sonatype					
nexus_repository_manager					
Exposure of Sensitive Information to an Unauthorized Actor	02-Nov-21	4	Sonatype Nexus Repository Manager 3.x through 3.35.0 allows attackers to access the SSL Certificates Loading function via a low-privileged account. **CVE ID : CVE-2021-42568**	https://support.sonatype.com, https://support.sonatype.com/hc/en-us/articles/4408801690515-CVE-2021-42568-Nexus-Repository-Manager-3-Incorrect-Access-Control-October-27-2021	A-SON-NEXU-181121/526
Server-Side Request Forgery (SSRF)	04-Nov-21	4	Sonatype Nexus Repository Manager 3.x before 3.36.0 allows a remote authenticated attacker to potentially perform network enumeration via Server Side Request Forgery (SSRF). **CVE ID : CVE-2021-43293**	https://support.sonatype.com/hc/en-us/articles/4409326330003	A-SON-NEXU-181121/527
spacewalk_project					
spacewalk					
Improper	01-Nov-21	9.3	Spacewalk 2.10, and	http://www.	A-SPA-SPAC-

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
Control of Generation of Code ('Code Injection')		🟥	derivatives such as Uyuni 2021.08, allows code injection. rhn-config-satellite.pl doesn't sanitize the configuration filename used to append Spacewalk-specific key-value pair. The script is intended to be run by the tomcat user account with Sudo, according to the installation setup. This can lead to the ability of an attacker to use --option to append arbitrary code to a root-owned file that eventually will be executed by the system. This is fixed in Uyuni spacewalk-admin 4.3.2-1. **CVE ID : CVE-2021-40348**	openwall.com/lists/oss-security/2021/10/28/4, https://github.com/uyuni-project/uyuni/commit/790c7388efac6923c5475e01c1ff718dffa9f052	181121/528
starkbank					
ecdsa-dotnet					
Improper Verification of Cryptographic Signature	09-Nov-21	7.5	The verify function in the Stark Bank .NET ECDSA library (ecdsa-dotnet) 1.3.1 fails to check that the signature is non-zero, which allows attackers to forge signatures on arbitrary messages. **CVE ID : CVE-2021-43569**	N/A	A-STA-ECDS-181121/529
ecdsa-java					
Improper Verification of Cryptographic Signature	09-Nov-21	7.5	The verify function in the Stark Bank Java ECDSA library (ecdsa-java) 1.0.0 fails to check that the signature is non-zero, which allows attackers to forge signatures on arbitrary	N/A	A-STA-ECDS-181121/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages. **CVE ID : CVE-2021-43570**		
ecdsa-node					
Improper Verification of Cryptographic Signature	09-Nov-21	7.5	The verify function in the Stark Bank Node.js ECDSA library (ecdsa-node) 1.1.2 fails to check that the signature is non-zero, which allows attackers to forge signatures on arbitrary messages. **CVE ID : CVE-2021-43571**	N/A	A-STA-ECDS-181121/531
ecdsa-python					
Improper Verification of Cryptographic Signature	09-Nov-21	7.5	The verify function in the Stark Bank Python ECDSA library (ecdsa-python) 2.0.0 fails to check that the signature is non-zero, which allows attackers to forge signatures on arbitrary messages. **CVE ID : CVE-2021-43572**	N/A	A-STA-ECDS-181121/532
elixir_ecdsa					
Improper Verification of Cryptographic Signature	09-Nov-21	7.5	The verify function in the Stark Bank Elixir ECDSA library (ecdsa-elixir) 1.0.0 fails to check that the signature is non-zero, which allows attackers to forge signatures on arbitrary messages. **CVE ID : CVE-2021-43568**	N/A	A-STA-ELIX-181121/533
stylishpricelist					
stylish_price_list					
Incorrect Authorization	01-Nov-21	5	The Stylish Price List WordPress plugin before 6.9.0 does not perform	N/A	A-STY-STYL-181121/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			capability checks in its spl_upload_ser_img AJAX action (available to both unauthenticated and authenticated users), which could allow unauthenticated users to upload images. **CVE ID : CVE-2021-24757**		
Incorrect Authorization	01-Nov-21	4	The Stylish Price List WordPress plugin before 6.9.1 does not perform capability checks in its spl_upload_ser_img AJAX action (available to authenticated users), which could allow any authenticated users, such as subscriber, to upload arbitrary images. **CVE ID : CVE-2021-24770**	N/A	A-STY-STYL-181121/535
supsystic					
easy_google_maps					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	2.1	The Google Maps Easy WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/modules/marker_groups/views/tpl/mgrEditMarkerGroup.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.9.33. This affects multi-site	https://plugins.trac.wordpress.org/changeset/2620851/google-maps-easy/trunk/modules/marker_groups/views/tpl/mgrEditMarkerGroup.php	A-SUP-EASY-181121/536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled. **CVE ID : CVE-2021-39346**		
tailor_management_system_project					
tailor_management_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	4.3	Multiple Cross Site Scripting (XSS) vulnerabilities exist in SourceCodester Tailor Management 1.0 via the (1) eid parameter in (a) partedit.php and (b) customeredit.php, the (2) id parameter in (a) editmeasurement.php and (b) addpayment.php, and the (3) error parameter in index.php. **CVE ID : CVE-2021-40260**	N/A	A-TAI-TAIL-181121/537
talend					
data_catalog					
Incorrect Authorization	05-Nov-21	7.5	An issue was discovered in Talend Data Catalog before 7.3-20210930. After setting up SAML/OAuth, authentication is not correctly enforced on the native login page. Any valid user from the SAML/OAuth provider can be used as the username with an arbitrary password, and login will succeed. **CVE ID : CVE-2021-42837**	https://www.talend.com/resources/, https://jira.talendforge.org/browse/TAPACHE-180	A-TAL-DATA-181121/538
tempura_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tempura					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-21	4.3	This affects the package tempura before 0.4.0. If the input to the esc function is of type object (i.e an array) it is returned without being escaped/sanitized, leading to a potential Cross-Site Scripting vulnerability. **CVE ID : CVE-2021-23784**	https://github.com/lukeed/tempura/commit/58a5c3671e2f36b26810e77ead9e0dd471902f9b, https://snyk.io/vuln/SNYK-JS-TEMPURA-1569633	A-TEM-TEMP-181121/539
Tenable					
nessus					
Improper Privilege Management	03-Nov-21	4.6	Nessus versions 8.15.2 and earlier were found to contain a local privilege escalation vulnerability which could allow an authenticated, local administrator to run specific executables on the Nessus Agent host. Tenable has included a fix for this issue in Nessus 10.0.0. The installation files can be obtained from the Tenable Downloads Portal (https://www.tenable.com/downloads/nessus). **CVE ID : CVE-2021-20135**	https://www.tenable.com/security/tns-2021-18	A-TEN-NESS-181121/540
thruk					
thruk					
Improper Neutralization of Input	09-Nov-21	4.3	Thruk 2.40-2 allows /thruk/#cgi-bin/status.cgi?style=combin	https://www.thruk.org/changelog.ht	A-THR-THRU-181121/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			ed&title={TITLE] Reflected XSS via the host or title parameter. An attacker could inject arbitrary JavaScript into status.cgi. The payload would be triggered every time an authenticated user browses the page containing it. **CVE ID : CVE-2021-35488**	ml	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-21	4.3	Thruk 2.40-2 allows /thruk/#cgi-bin/extinfo.cgi?type=2&host={HOSTNAME]&service={SERVICENAME]&backend={BACKEND] Reflected XSS via the host or service parameter. An attacker could inject arbitrary JavaScript into extinfo.cgi. The malicious payload would be triggered every time an authenticated user browses the page containing it. **CVE ID : CVE-2021-35489**	https://www.thruk.org/changelog.html	A-THR-THRU-181121/542
thunderdome					
planning_poker					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-Nov-21	7.5	Thunderdome is an open source agile planning poker tool in the theme of Battling for points. In affected versions there is an LDAP injection vulnerability which affects instances with LDAP authentication enabled. The provided username is not properly escaped. This issue has	https://github.com/StevenWeathers/thunderdome-planning-poker/security/advisories/GHSA-26cm-qrc6-mfgj,	A-THU-PLAN-181121/543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			been patched in version 1.16.3. If users are unable to update they should disable the LDAP feature if in use. **CVE ID : CVE-2021-41232**	https://github.com/StevenWeathers/thunderdome-planning-poker/commit/f1524d01e8a0f2d6c3db5461c742456c692dd8c1	
Tipsandtricks-hq					
far_future_expiry_header					
Cross-Site Request Forgery (CSRF)	01-Nov-21	4.3	The Far Future Expiry Header WordPress plugin before 1.5 does not have CSRF check when saving its settings, which could allow attackers to make a logged in admin change them via a CSRF attack. **CVE ID : CVE-2021-24799**	N/A	A-TIP-FAR_-181121/544
simple_download_monitor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	6	The Simple Download Monitor WordPress plugin before 3.9.5 does not escape the "File Thumbnail" post meta before outputting it in some pages, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks. Given the that XSS is triggered even when the Download is in a review state, contributor could make JavaScript code execute in a context of a	N/A	A-TIP-SIMP-181121/545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reviewer such as admin and make them create a rogue admin account, or install a malicious plugin **CVE ID : CVE-2021-24693**		
Exposure of Sensitive Information to an Unauthorized Actor	08-Nov-21	5	The Simple Download Monitor WordPress plugin before 3.9.6 saves logs in a predictable location, and does not have any authentication or authorisation in place to prevent unauthenticated users to download and read the logs containing Sensitive Information such as IP Addresses and Usernames **CVE ID : CVE-2021-24695**	N/A	A-TIP-SIMP-181121/546
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	4.3	The Simple Download Monitor WordPress plugin before 3.9.5 does not escape the 1) sdm_active_tab GET parameter and 2) sdm_stats_start_date/sdm_stats_end_date POST parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting issues **CVE ID : CVE-2021-24697**	N/A	A-TIP-SIMP-181121/547
N/A	08-Nov-21	4	The Simple Download Monitor WordPress plugin before 3.9.6 allows users with a role as low as Contributor to remove thumbnails from downloads they do not own, even if	N/A	A-TIP-SIMP-181121/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			they cannot normally edit the download. **CVE ID : CVE-2021-24698**		
unicode					
unicode					
Improper Control of Generation of Code ('Code Injection')	01-Nov-21	7.5	An issue was discovered in the Bidirectional Algorithm in the Unicode Specification through 14.0. It permits the visual reordering of characters via control sequences, which can be used to craft source code that renders different logic than the logical ordering of tokens ingested by compilers and interpreters. Adversaries can leverage this to encode source code for compilers accepting Unicode such that targeted vulnerabilities are introduced invisibly to human reviewers. **CVE ID : CVE-2021-42574**	http://www.unicode.org/versions/Unicode14.0.0/	A-UNI-UNIC-181121/549
Improper Control of Generation of Code ('Code Injection')	01-Nov-21	7.5	An issue was discovered in the character definitions of the Unicode Specification through 14.0. The specification allows an adversary to produce source code identifiers such as function names using homoglyphs that render visually identical to a target identifier. Adversaries can leverage this to inject code via adversarial identifier definitions in upstream	http://www.unicode.org/versions/Unicode14.0.0/	A-UNI-UNIC-181121/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			software dependencies invoked deceptively in downstream software. **CVE ID : CVE-2021-42694**		
unlimited_popups_project					
unlimited_popups					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	6.5	The Unlimited PopUps WordPress plugin through 4.5.3 does not sanitise or escape the did GET parameter before using it in a SQL statement, available to users as low as editor, leading to an authenticated SQL Injection **CVE ID : CVE-2021-24631**	N/A	A-UNL-UNLI-181121/551
uyuni_project					
uyuni					
Improper Control of Generation of Code ('Code Injection')	01-Nov-21	9.3	Spacewalk 2.10, and derivatives such as Uyuni 2021.08, allows code injection. rhn-config-satellite.pl doesn't sanitize the configuration filename used to append Spacewalk-specific key-value pair. The script is intended to be run by the tomcat user account with Sudo, according to the installation setup. This can lead to the ability of an attacker to use --option to append arbitrary code to a root-owned file that eventually will be executed by the system. This is fixed in Uyuni spacewalk-admin 4.3.2-1.	http://www.openwall.com/lists/oss-security/2021/10/28/4, https://github.com/uyuni-project/uyuni/commit/790c7388efac6923c5475e01c1ff718dffa9f052	A-UYU-UYUN-181121/552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40348		
Vaadin					
vaadin					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-21	4.3	Missing output sanitization in test sources in org.webjars.bowergithub.vaadin:vaadin-menu-bar versions 1.0.0 through 1.2.0 (Vaadin 14.0.0 through 14.4.4) allows remote attackers to execute malicious JavaScript in browser by opening crafted URL **CVE ID : CVE-2021-33611**	https://vaadin.com/security/cve-2021-33611, https://github.com/vaadin/vaadin-menu-bar/pull/126	A-VAA-VAAD-181121/553
vaadin-menu-bar					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-21	4.3	Missing output sanitization in test sources in org.webjars.bowergithub.vaadin:vaadin-menu-bar versions 1.0.0 through 1.2.0 (Vaadin 14.0.0 through 14.4.4) allows remote attackers to execute malicious JavaScript in browser by opening crafted URL **CVE ID : CVE-2021-33611**	https://vaadin.com/security/cve-2021-33611, https://github.com/vaadin/vaadin-menu-bar/pull/126	A-VAA-VAAD-181121/554
validator_project					
validator					
N/A	02-Nov-21	5	validator.js is vulnerable to Inefficient Regular Expression Complexity **CVE ID : CVE-2021-3765**	https://huntr.dev/bounties/c37e975c-21a3-4c5f-9b57-04d63b28cfc9, https://gith	A-VAL-VALI-181121/555

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
				ub.com/validatorjs/validator.js/commit/496fc8b2a7f5997acaaec33cc44d0b8dba5fb5e1	
vfront					
vfront					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	4.3	Multiple Cross Site Scripting (XSS) vulnerabilities exist in VFront 0.99.5 via the (1) s parameter in search_all.php and the (2) msg parameter in add.attach.php. **CVE ID : CVE-2021-39420**	N/A	A-VFR-VFRO-181121/556
VIM					
vim					
Heap-based Buffer Overflow	05-Nov-21	6.8	vim is vulnerable to Heap-based Buffer Overflow **CVE ID : CVE-2021-3927**	https://huntr.dev/bounties/9c2b2c82-48bb-4be9-ab8f-a48ea252d1b0, https://github.com/vim/vim/commit/0b5b06cb4777d1401fdf83e7d48d287662236e7e	A-VIM-VIM-181121/557
Stack-based Buffer Overflow	05-Nov-21	4.6	vim is vulnerable to Stack-based Buffer Overflow **CVE ID : CVE-2021-3928**	https://huntr.dev/bounties/29c3ebd2-d601-	A-VIM-VIM-181121/558

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
				481c-bf96-76975369d0cd, https://github.com/vim/vim/commit/15d9890eee53afc61eb0a03b878a19cb5672f732	
Vmware					
spring_cloud_gateway					
Incorrect Authorization	08-Nov-21	4	Applications using Spring Cloud Gateway are vulnerable to specifically crafted requests that could make an extra request on downstream services. Users of affected versions should apply the following mitigation: 3.0.x users should upgrade to 3.0.5+, 2.2.x users should upgrade to 2.2.10.RELEASE or newer. **CVE ID : CVE-2021-22051**	https://tanzu.vmware.com/security/cve-2021-22051	A-VMW-SPRI-181121/559
wclovers					
frontend_manager_for_woocommerce_along_with_bookings_subscription_listings_compatible					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	08-Nov-21	6.5	The WCFM â€“ Frontend Manager for WooCommerce along with Bookings Subscription Listings Compatible WordPress plugin before 6.5.12, when used in combination with another WCFM - WooCommerce	N/A	A-WCL-FRON-181121/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			Multivendor plugin such as WCFM - WooCommerce Multivendor Marketplace, does not escape the withdrawal_vendor parameter before using it in a SQL statement, allowing low privilege users such as Subscribers to perform SQL injection attacks **CVE ID : CVE-2021-24835**		
Web-dorado					
spidercatalog					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	6.5	The SpiderCatalog WordPress plugin through 1.7.3 does not sanitise or escape the 'parent' and 'ordering' parameters from the admin dashboard before using them in a SQL statement, leading to a SQL injection when adding a category **CVE ID : CVE-2021-24625**	N/A	A-WEB-SPID-181121/561
webnus					
modern_events_calendar_lite					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	3.5	The Modern Events Calendar Lite WordPress plugin before 5.22.3 does not properly sanitize or escape values set by users with access to adjust settings withing wp-admin. **CVE ID : CVE-2021-24716**	N/A	A-WEB-MODE-181121/562
wooassist					
storefront_footer_text					
Improper	08-Nov-21	3.5	The Storefront Footer Text	N/A	A-WOO-STOR-

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
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			WordPress plugin through 1.0.1 does not sanitize and escape the "Footer Credit Text" added to pages, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered-html capability is disallowed. **CVE ID : CVE-2021-24607**		181121/563
wordplus					
better_messages					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	4.3	The BP Better Messages WordPress plugin before 1.9.9.41 sanitise (with sanitize_text_field) but does not escape the 'subject' parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24808**	https://plugins.trac.wordpress.org/changeset/2605772/bp-better-messages/trunk/views/layout-new.php	A-WOR-BETT-181121/564
Cross-Site Request Forgery (CSRF)	01-Nov-21	6.8	The BP Better Messages WordPress plugin before 1.9.9.41 does not check for CSRF in multiple of its AJAX actions: bp_better_messages_leave_chat, bp_better_messages_join_chat, bp_messages_leave_thread, bp_messages_mute_thread, bp_messages_unmute_thread, bp_better_messages_add_user_to_thread, bp_better_messages_exclud	https://plugins.trac.wordpress.org/changeset/2605772/bp-better-messages/trunk/inc/ajax.php	A-WOR-BETT-181121/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			e_user_from_thread. This could allow attackers to make logged in users do unwanted actions **CVE ID : CVE-2021-24809**		
wow-company					
wow_forms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	6.5	The Wow Forms WordPress plugin through 3.1.3 does not sanitise or escape a 'did' GET parameter before using it in a SQL statement, when deleting a form in the admin dashboard, leading to an authenticated SQL injection **CVE ID : CVE-2021-24628**	N/A	A-WOW-WOW_-181121/566
wp-buy					
visitor_traffic_real_time_statistics					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Nov-21	6.5	The Visitor Traffic Real Time Statistics WordPress plugin before 3.9 does not validate and escape user input passed to the today_traffic_index AJAX action (available to any authenticated users) before using it in a SQL statement, leading to an SQL injection issue **CVE ID : CVE-2021-24829**	N/A	A-WP--VISI-181121/567
wpaffiliatemanager					
affiliates_manager					
Improper Neutralization of Special Elements used in an	08-Nov-21	6.5	The Affiliates Manager WordPress plugin before 2.8.7 does not validate the orderby parameter before using it in an SQL statement	https://plugins.trac.wordpress.org/changeset/2611862/	A-WPA-AFFI-181121/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			in the admin dashboard, leading to an SQL Injection issue **CVE ID : CVE-2021-24844**		
wpdownloadmanager					
wordpress_download_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	3.5	The WordPress Download Manager WordPress plugin before 3.2.16 does not escape some of the Download settings when outputting them, allowing high privilege users to perform XSS attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24773**	N/A	A-WPD-WORD-181121/569
wpkube					
cool_tag_cloud					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	3.5	The Cool Tag Cloud WordPress plugin before 2.26 does not escape the style attribute of the cool_tag_cloud shortcode, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2021-24682**	N/A	A-WPK-COOL-181121/570
wpplugin					
accept_donations_with_paypal					
Cross-Site Request Forgery (CSRF)	01-Nov-21	4.3	The Accept Donations with PayPal WordPress plugin before 1.3.1 offers a function to create donation buttons, which internally	https://plugins.trac.wordpress.org/changeset/2608073/	A-WPP-ACCE-181121/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are posts. The process to create a new button is lacking a CSRF check. An attacker could use this to make an authenticated admin create a new button. Furthermore, one of the Button field is not escaped before being output in an attribute when editing a Button, leading to a Stored Cross-Site Scripting issue as well. **CVE ID : CVE-2021-24570**		
Cross-Site Request Forgery (CSRF)	01-Nov-21	4.3	The Accept Donations with PayPal WordPress plugin before 1.3.1 provides a function to create donation buttons which are internally stored as posts. The deletion of a button is not CSRF protected and there is no control to check if the deleted post was a button post. As a result, an attacker could make logged in admins delete arbitrary posts **CVE ID : CVE-2021-24572**	N/A	A-WPP-ACCE-181121/572
wpreactions					
wp_reactions_lite					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	3.5	The WP Reactions Lite WordPress plugin before 1.3.6 does not properly sanitize inputs within wp-admin pages, allowing users with sufficient access to inject XSS payloads within /wp-admin/ pages.	N/A	A-WPR-WP_R-181121/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24723		
wp_all_export_project					
wp_all_export					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	3.5	The Export any WordPress data to XML/CSV WordPress plugin before 1.3.1 does not escape its Export's Name before outputting it in Manage Exports settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24708**	N/A	A-WP_-WP_A-181121/574
wp_seo_redirect_301_project					
wp_seo_redirect_301					
Cross-Site Request Forgery (CSRF)	08-Nov-21	4.3	The WP SEO Redirect 301 WordPress plugin before 2.3.2 does not have CSRF in place when deleting redirects, which could allow attackers to make a logged in admin delete them via a CSRF attack **CVE ID : CVE-2021-24832**	N/A	A-WP_-WP_S-181121/575
wp_sitemap_page_project					
wp_sitemap_page					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	3.5	The WP Sitemap Page WordPress plugin before 1.7.0 does not properly sanitise and escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when	N/A	A-WP_-WP_S-181121/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24715**		
wp_survey_plus_project					
wp_survey_plus					
Cross-Site Request Forgery (CSRF)	08-Nov-21	4.3	The WP Survey Plus WordPress plugin through 1.0 does not have any authorisation and CSRF checks in place in its AJAX actions, allowing any user to call them and add/edit/delete Surveys. Furthermore, due to the lack of sanitization in the Surveys' Title, this could also lead to Stored Cross-Site Scripting issues **CVE ID : CVE-2021-24801**	N/A	A-WP_-WP_S-181121/577
xenforo					
xenforo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-21	3.5	In XenForo through 2.2.7, a threat actor with access to the admin panel can create a new Advertisement via the Advertising function, and save an XSS payload in the body of the HTML document. This payload will execute globally on the client side. **CVE ID : CVE-2021-43032**	https://xenforo.com/community/forums/announcements/	A-XEN-XENF-181121/578
xorux					
lpar2rrd					
Cleartext Storage of Sensitive	08-Nov-21	4.3	A password mismanagement situation exists in XoruX LPAR2RRD	https://stor2rrd.com/note730.php,	A-XOR-LPAR-181121/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information			and STOR2RRD before 7.30 because cleartext information is present in HTML password input fields in the device properties. (Viewing the passwords requires configuring a web browser to display HTML password input fields.) **CVE ID : CVE-2021-42370**	https://lpar2rrd.com/note730.php	
Insecure Storage of Sensitive Information	08-Nov-21	7.5	lpar2rrd is a hardcoded system account in XoruX LPAR2RRD and STOR2RRD before 7.30. **CVE ID : CVE-2021-42371**	https://stor2rrd.com/note730.php, https://lpar2rrd.com/note730.php	A-XOR-LPAR-181121/580
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Nov-21	9	A shell command injection in the HW Events SNMP community in XoruX LPAR2RRD and STOR2RRD before 7.30 allows authenticated remote attackers to execute arbitrary shell commands as the user running the service. **CVE ID : CVE-2021-42372**	https://stor2rrd.com/note730.php, https://lpar2rrd.com/note730.php	A-XOR-LPAR-181121/581
stor2rrd					
Cleartext Storage of Sensitive Information	08-Nov-21	4.3	A password mismanagement situation exists in XoruX LPAR2RRD and STOR2RRD before 7.30 because cleartext information is present in HTML password input fields in the device properties. (Viewing the passwords requires configuring a web browser to display HTML	https://stor2rrd.com/note730.php, https://lpar2rrd.com/note730.php	A-XOR-STOR-181121/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			password input fields.) **CVE ID : CVE-2021-42370**		
Insecure Storage of Sensitive Information	08-Nov-21	7.5	lpar2rrd is a hardcoded system account in XoruX LPAR2RRD and STOR2RRD before 7.30. **CVE ID : CVE-2021-42371**	https://stor2rrd.com/note730.php, https://lpar2rrd.com/note730.php	A-XOR-STOR-181121/583
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Nov-21	9	A shell command injection in the HW Events SNMP community in XoruX LPAR2RRD and STOR2RRD before 7.30 allows authenticated remote attackers to execute arbitrary shell commands as the user running the service. **CVE ID : CVE-2021-42372**	https://stor2rrd.com/note730.php, https://lpar2rrd.com/note730.php	A-XOR-STOR-181121/584
youphptube					
youphptube					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-21	5	AVideo/YouPHPTube AVideo/YouPHPTube 10.0 and prior is affected by a SQL Injection SQL injection in the catName parameter which allows a remote unauthenticated attacker to retrieve databases information such as application passwords hashes. **CVE ID : CVE-2021-25874**	https://www.synacktiv.com/sites/default/files/2021-01/YouPHPTube_Multiple_Vulnerabilities.pdf	A-YOU-YOUP-181121/585
Improper Neutralization of Input During Web Page	01-Nov-21	4.3	AVideo/YouPHPTube AVideo/YouPHPTube 10.0 and prior has multiple reflected Cross Script Scripting vulnerabilities via	https://www.synacktiv.com/sites/default/files/2021-	A-YOU-YOUP-181121/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			the searchPhrase parameter which allows a remote attacker to steal administrators' session cookies or perform actions as an administrator. **CVE ID : CVE-2021-25875**	01/YouPHPTube_Multiple_Vulnerabilities.pdf	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	4.3	AVideo/YouPHPTube 10.0 and prior has multiple reflected Cross Script Scripting vulnerabilities via the u parameter which allows a remote attacker to steal administrators' session cookies or perform actions as an administrator. **CVE ID : CVE-2021-25876**	https://www.synacktiv.com/sites/default/files/2021-01/YouPHPTube_Multiple_Vulnerabilities.pdf	A-YOU-YOUP-181121/587
Incorrect Permission Assignment for Critical Resource	01-Nov-21	9	AVideo/YouPHPTube 10.0 and prior is affected by Insecure file write. An administrator privileged user is able to write files on filesystem using flag and code variables in file save.php. **CVE ID : CVE-2021-25877**	https://www.synacktiv.com/sites/default/files/2021-01/YouPHPTube_Multiple_Vulnerabilities.pdf	A-YOU-YOUP-181121/588
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-21	4.3	AVideo/YouPHPTube 10.0 and prior is affected by multiple reflected Cross Script Scripting vulnerabilities via the videoName parameter which allows a remote attacker to steal administrators' session cookies or perform actions as an administrator. **CVE ID : CVE-2021-25878**	https://www.synacktiv.com/sites/default/files/2021-01/YouPHPTube_Multiple_Vulnerabilities.pdf	A-YOU-YOUP-181121/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Zohocorp					
manageengine_log360					
Incorrect Authorization	01-Nov-21	7.5	ManageEngine Log360 Builds < 5235 are affected by an improper access control vulnerability allowing database configuration overwrite. An unauthenticated remote attacker can send a specially crafted message to Log360 to change its backend database to an attacker-controlled database and to force Log360 to restart. An attacker can leverage this vulnerability to achieve remote code execution by replacing files executed by Log360 on startup. **CVE ID : CVE-2021-20136**	N/A	A-ZOH-MANA-181121/590
Hardware					
airangel					
hsmx-app-100					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-21	3.5	Airangel HSMX Gateway devices through 5.2.04 is vulnerable to stored Cross Site Scripting. XSS Payload is placed in the name column of the updates table using database access. **CVE ID : CVE-2021-40517**	N/A	H-AIR-HSMX-221121/591
Use of Hard-coded Credentials	10-Nov-21	6.4	Airangel HSMX Gateway devices through 5.2.04 have Hard-coded Database Credentials. **CVE ID : CVE-2021-40519**	N/A	H-AIR-HSMX-221121/592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Nov-21	10	Airangel HSMX Gateway devices through 5.2.04 allow Remote Code Execution. **CVE ID : CVE-2021-40521**	N/A	H-AIR-HSMX-221121/593
hsmx-app-1000					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-21	3.5	Airangel HSMX Gateway devices through 5.2.04 is vulnerable to stored Cross Site Scripting. XSS Payload is placed in the name column of the updates table using database access. **CVE ID : CVE-2021-40517**	N/A	H-AIR-HSMX-221121/594
Use of Hard-coded Credentials	10-Nov-21	6.4	Airangel HSMX Gateway devices through 5.2.04 have Hard-coded Database Credentials. **CVE ID : CVE-2021-40519**	N/A	H-AIR-HSMX-221121/595
N/A	10-Nov-21	10	Airangel HSMX Gateway devices through 5.2.04 allow Remote Code Execution. **CVE ID : CVE-2021-40521**	N/A	H-AIR-HSMX-221121/596
hsmx-app-20000					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-21	3.5	Airangel HSMX Gateway devices through 5.2.04 is vulnerable to stored Cross Site Scripting. XSS Payload is placed in the name column of the updates table using database access. **CVE ID : CVE-2021-40517**	N/A	H-AIR-HSMX-221121/597
Use of Hard-coded Credentials	10-Nov-21	6.4	Airangel HSMX Gateway devices through 5.2.04 have Hard-coded Database Credentials.	N/A	H-AIR-HSMX-221121/598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40519		
N/A	10-Nov-21	10	Airangel HSMX Gateway devices through 5.2.04 allow Remote Code Execution. **CVE ID : CVE-2021-40521**	N/A	H-AIR-HSMX-221121/599
hsmx-app-25					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-21	3.5	Airangel HSMX Gateway devices through 5.2.04 is vulnerable to stored Cross Site Scripting. XSS Payload is placed in the name column of the updates table using database access. **CVE ID : CVE-2021-40517**	N/A	H-AIR-HSMX-221121/600
Use of Hard-coded Credentials	10-Nov-21	6.4	Airangel HSMX Gateway devices through 5.2.04 have Hard-coded Database Credentials. **CVE ID : CVE-2021-40519**	N/A	H-AIR-HSMX-221121/601
N/A	10-Nov-21	10	Airangel HSMX Gateway devices through 5.2.04 allow Remote Code Execution. **CVE ID : CVE-2021-40521**	N/A	H-AIR-HSMX-221121/602
hsmx-app-5000					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-21	3.5	Airangel HSMX Gateway devices through 5.2.04 is vulnerable to stored Cross Site Scripting. XSS Payload is placed in the name column of the updates table using database access. **CVE ID : CVE-2021-40517**	N/A	H-AIR-HSMX-221121/603
Use of Hard-coded Credentials	10-Nov-21	6.4	Airangel HSMX Gateway devices through 5.2.04 have Hard-coded Database	N/A	H-AIR-HSMX-221121/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Credentials. **CVE ID : CVE-2021-40519**		
N/A	10-Nov-21	10	Airangel HSMX Gateway devices through 5.2.04 allow Remote Code Execution. **CVE ID : CVE-2021-40521**	N/A	H-AIR-HSMX-221121/605
Beckhoff					
tf6100					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Nov-21	8.5	TwinCAT OPC UA Server in TF6100 and TS6100 in product versions before 4.3.48.0 or with TcOpcUaServer versions below 3.2.0.194 are prone to a relative path traversal that allow administrators to create or delete any files on the system. **CVE ID : CVE-2021-34594**	https://cert.vde.com/en/advisories/VDE-2021-051/	H-BEC-TF61-221121/606
ts6100					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Nov-21	8.5	TwinCAT OPC UA Server in TF6100 and TS6100 in product versions before 4.3.48.0 or with TcOpcUaServer versions below 3.2.0.194 are prone to a relative path traversal that allow administrators to create or delete any files on the system. **CVE ID : CVE-2021-34594**	https://cert.vde.com/en/advisories/VDE-2021-051/	H-BEC-TS61-221121/607
beeline					
smart_box					
Cross-Site Request Forgery	10-Nov-21	6.8	Beeline Smart box 2.0.38 is vulnerable to Cross Site Request Forgery (CSRF) via	https://tula.beeline.ru/customers/po	H-BEE-SMAR-221121/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			mgt_end_user.htm. **CVE ID : CVE-2021-41426**	mosh/home/domashnij-internet/nastrojki-s-routerom/beelinesmartbox/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-21	4.3	Beeline Smart Box 2.0.38 is vulnerable to Cross Site Scripting (XSS) via the choose_mac parameter to setup.cgi. **CVE ID : CVE-2021-41427**	https://tula.beeline.ru/customers/pomosh/home/domashnij-internet/nastrojki-s-routerom/beelinesmartbox/	H-BEE-SMAR-221121/609
Cisco					
catalyst_pon_switch_cgp-ont-1p					
Use of Hard-coded Credentials	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34795**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	04-Nov-21	5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40112**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/611
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40113**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
catalyst_pon_switch_cgp-ont-4p					
Use of Hard-coded Credentials	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34795**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/613
Improper Input Validation	04-Nov-21	5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40112		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40113**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/615
catalyst_pon_switch_cgp-ont-4pv					
Use of Hard-coded Credentials	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			advisory. **CVE ID : CVE-2021-34795**		
Improper Input Validation	04-Nov-21	5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40112**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/617
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			advisory. **CVE ID : CVE-2021-40113**		
catalyst_pon_switch_cgp-ont-4pvc					
Use of Hard-coded Credentials	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34795**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/619
Improper Input Validation	04-Nov-21	5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40112**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40113**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/621
catalyst_pon_switch_cgp-ont-4tvcw					
Use of Hard-coded Credentials	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34795**		
Improper Input Validation	04-Nov-21	5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40112**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/623
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	H-CIS-CATA-221121/624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40113**		
rv016					
Improper Input Validation	04-Nov-21	9	A vulnerability in the web-based management interface of certain Cisco Small Business RV Series Routers could allow an authenticated, remote attacker with administrative privileges to inject arbitrary commands into the underlying operating system and execute them using root-level privileges. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to a specific field in the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as a user with root-level privileges. **CVE ID : CVE-2021-40120**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-cmdinjection-Z5cWFdK	H-CIS-RV01-221121/625
rv042					
Improper Input	04-Nov-21	9	A vulnerability in the web-based management	https://tools.cisco.com/s	H-CIS-RV04-221121/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			interface of certain Cisco Small Business RV Series Routers could allow an authenticated, remote attacker with administrative privileges to inject arbitrary commands into the underlying operating system and execute them using root-level privileges. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to a specific field in the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as a user with root-level privileges. **CVE ID : CVE-2021-40120**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-cmdinjection-Z5cWFdK	
rv042g					
Improper Input Validation	04-Nov-21	9	A vulnerability in the web-based management interface of certain Cisco Small Business RV Series Routers could allow an authenticated, remote attacker with administrative privileges to inject arbitrary commands into the underlying operating system and execute them using root-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-cmdinjection-Z5cWFdK	H-CIS-RV04-221121/627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			level privileges. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to a specific field in the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as a user with root-level privileges. **CVE ID : CVE-2021-40120**		
rv082					
Improper Input Validation	04-Nov-21	9	A vulnerability in the web-based management interface of certain Cisco Small Business RV Series Routers could allow an authenticated, remote attacker with administrative privileges to inject arbitrary commands into the underlying operating system and execute them using root-level privileges. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to a specific field in the web-based management interface of an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-cmdinjection-Z5cWFdK	H-CIS-RV08-221121/628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as a user with root-level privileges. **CVE ID : CVE-2021-40120**		
rv320					
Improper Input Validation	04-Nov-21	9	A vulnerability in the web-based management interface of certain Cisco Small Business RV Series Routers could allow an authenticated, remote attacker with administrative privileges to inject arbitrary commands into the underlying operating system and execute them using root-level privileges. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to a specific field in the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as a user with root-level privileges. **CVE ID : CVE-2021-40120**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-cmdinjection-Z5cWFdK	H-CIS-RV32-221121/629
rv325					
Improper	04-Nov-21	9	A vulnerability in the web-	https://tools	H-CIS-RV32-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			based management interface of certain Cisco Small Business RV Series Routers could allow an authenticated, remote attacker with administrative privileges to inject arbitrary commands into the underlying operating system and execute them using root-level privileges. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to a specific field in the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as a user with root-level privileges. **CVE ID : CVE-2021-40120**	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-cmdinjection-Z5cWFdK	221121/630
sf200-24					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF20-221121/631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf200-24fp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF20-221121/632

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
			could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf200-24p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF20-221121/633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf200-48					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF20-221121/634
sf200-48p					
Improper Input	04-Nov-21	5	A vulnerability in the web-based management	https://tools.cisco.com/s	H-CIS-SF20-221121/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	
sf200e-24					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF20-221121/636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf200e-24p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF20-221121/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf200e-48					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF20-221121/638

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
			for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf200e-48p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF20-221121/639
sf300-08					
Improper	04-Nov-21	5	A vulnerability in the web-	https://tools	H-CIS-SF30-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	221121/640
sf300-24					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-	H-CIS-SF30-221121/641

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
			Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	xMyFFkt8	
sf300-24mp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF30-221121/642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf300-24p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF30-221121/643

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
			permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf300-24pp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF30-221121/644
sf300-48					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF30-221121/645
sf300-48p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-	H-CIS-SF30-221121/646

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
			Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	web-dos-xMyFFkt8	
sf300-48pp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF30-221121/647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf302-08					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF30-221121/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf302-08mp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF30-221121/649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf302-08mpp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF30-221121/650
sf302-08p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	H-CIS-SF30-221121/651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sf302-08pp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF30-221121/652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf500-24					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF50-221121/653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf500-24mp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF50-221121/654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf500-24p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF50-221121/655
sf500-48					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	H-CIS-SF50-221121/656

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
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sf500-48mp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF50-221121/657

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
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf500-48p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SF50-221121/658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg200-08					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG20-221121/659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg200-08p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG20-221121/660
sg200-10fp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	H-CIS-SG20-221121/661

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
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg200-18					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG20-221121/662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg200-26					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG20-221121/663

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
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg200-26fp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG20-221121/664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg200-26p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG20-221121/665
sg200-50					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	H-CIS-SG20-221121/666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg200-50fp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG20-221121/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg200-50p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG20-221121/668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg300-10					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG30-221121/669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-10mp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG30-221121/670
sg300-10mpp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	H-CIS-SG30-221121/671

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
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg300-10p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG30-221121/672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg300-10pp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG30-221121/673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg300-20					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG30-221121/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-28					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG30-221121/675
sg300-28mp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	H-CIS-SG30-221121/676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg300-28p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG30-221121/677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg300-28pp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG30-221121/678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg300-28sfp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG30-221121/679

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
sg300-52					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG30-221121/680
sg300-52mp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	H-CIS-SG30-221121/681

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
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg300-52p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG30-221121/682

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
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg300-sfp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG30-221121/683

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
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg500-28					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG50-221121/684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg500-28mpp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG50-221121/685
sg500-28p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	H-CIS-SG50-221121/686

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
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg500-52					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG50-221121/687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg500-52mp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG50-221121/688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg500-52p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG50-221121/689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg500x-24					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG50-221121/690
sg500x-24mpp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	H-CIS-SG50-221121/691

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
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg500x-24p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG50-221121/692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg500x-48					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG50-221121/693

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
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg500x-48mpp					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG50-221121/694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg500x-48p					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	H-CIS-SG50-221121/695
sg500xg-8f8t					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	H-CIS-SG50-221121/696

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
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
HP					
laserjet_pro_j8h60a					
Uncontrolled Resource Consumption	01-Nov-21	7.8	Potential security vulnerabilities have been discovered on a certain HP LaserJet Pro printer that may allow a Denial of Service on the device. **CVE ID : CVE-2021-3704**	https://support.hp.com/us-en/document/ish_4411563-4411589-16/hpsbpi03741	H-HP-LASE-221121/697
Incorrect Authorization	01-Nov-21	10	Potential security vulnerabilities have been discovered on a certain HP LaserJet Pro printer that	https://support.hp.com/us-en/documen	H-HP-LASE-221121/698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may allow an unauthorized user to reconfigure, reset the device. **CVE ID : CVE-2021-3705**	t/ish_4411563-4411589-16/hpsbpi03741	
laserjet_pro_j8h61a					
Uncontrolled Resource Consumption	01-Nov-21	7.8	Potential security vulnerabilities have been discovered on a certain HP LaserJet Pro printer that may allow a Denial of Service on the device. **CVE ID : CVE-2021-3704**	https://support.hp.com/us-en/document/ish_4411563-4411589-16/hpsbpi03741	H-HP-LASE-221121/699
Incorrect Authorization	01-Nov-21	10	Potential security vulnerabilities have been discovered on a certain HP LaserJet Pro printer that may allow an unauthorized user to reconfigure, reset the device. **CVE ID : CVE-2021-3705**	https://support.hp.com/us-en/document/ish_4411563-4411589-16/hpsbpi03741	H-HP-LASE-221121/700
hpe					
proliant_dl20_gen10_server					
N/A	01-Nov-21	7.2	A potential local bypass of security restrictions vulnerability has been identified in HPE ProLiant DL20 Gen10, HPE ProLiant ML30 Gen10, and HPE ProLiant MicroServer Gen10 Plus server's system ROMs prior to version 2.52. The vulnerability could be locally exploited to cause disclosure of sensitive information, denial of	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04197en_us	H-HPE-PROL-221121/701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS), and/or compromise system integrity. **CVE ID : CVE-2021-29213**		
proliant_microserver_gen10_plus					
N/A	01-Nov-21	7.2	A potential local bypass of security restrictions vulnerability has been identified in HPE ProLiant DL20 Gen10, HPE ProLiant ML30 Gen10, and HPE ProLiant MicroServer Gen10 Plus server's system ROMs prior to version 2.52. The vulnerability could be locally exploited to cause disclosure of sensitive information, denial of service (DoS), and/or compromise system integrity. **CVE ID : CVE-2021-29213**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04197en_us	H-HPE-PROL-221121/702
proliant_ml30_gen10_server					
N/A	01-Nov-21	7.2	A potential local bypass of security restrictions vulnerability has been identified in HPE ProLiant DL20 Gen10, HPE ProLiant ML30 Gen10, and HPE ProLiant MicroServer Gen10 Plus server's system ROMs prior to version 2.52. The vulnerability could be locally exploited to cause disclosure of sensitive information, denial of service (DoS), and/or compromise system integrity.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04197en_us	H-HPE-PROL-221121/703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29213		
meross					
mss550x					
Missing Encryption of Sensitive Data	05-Nov-21	4.3	Meross Smart Wi-Fi 2 Way Wall Switch (MSS550X), on its 3.1.3 version and before, creates an open Wi-Fi Access Point without the required security measures in its initial setup. This could allow a remote attacker to obtain the Wi-Fi SSID as well as the password configured by the user from Meross app via Http/JSON plain request. **CVE ID : CVE-2021-3774**	https://www.incibe-cert.es/en/early-warning/security-advisories/meross-mss550x-missing-encryption-sensitive-data	H-MER-MSS5-221121/704
Realtek					
rtl8195am					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Nov-21	7.5	A buffer overflow was discovered on Realtek RTL8195AM devices before 2.0.10. It exists in the client code when processing a malformed IE length of HT capability information in the Beacon and Association response frame. **CVE ID : CVE-2021-43573**	https://realtek.com	H-REA-RTL8-221121/705
Samsung					
exynos					
Improper Input Validation	05-Nov-21	4.6	Improper input validation vulnerability in HDCP prior to SMR Nov-2021 Release 1 allows attackers to arbitrary code execution. **CVE ID : CVE-2021-25503**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&m	H-SAM-EXYN-221121/706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				onth=11	
exynos_2100					
Improper Input Validation	05-Nov-21	2.1	A missing input validation in HDCP LDFW prior to SMR Nov-2021 Release 1 allows attackers to overwrite TZASC allowing TEE compromise. **CVE ID : CVE-2021-25500**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=11	H-SAM-EXYN-221121/707
exynos_980					
Improper Input Validation	05-Nov-21	2.1	A missing input validation in HDCP LDFW prior to SMR Nov-2021 Release 1 allows attackers to overwrite TZASC allowing TEE compromise. **CVE ID : CVE-2021-25500**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=11	H-SAM-EXYN-221121/708
exynos_9820					
Improper Input Validation	05-Nov-21	2.1	A missing input validation in HDCP LDFW prior to SMR Nov-2021 Release 1 allows attackers to overwrite TZASC allowing TEE compromise. **CVE ID : CVE-2021-25500**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=11	H-SAM-EXYN-221121/709
exynos_9830					
Improper Input Validation	05-Nov-21	2.1	A missing input validation in HDCP LDFW prior to SMR Nov-2021 Release 1 allows attackers to overwrite TZASC allowing TEE compromise. **CVE ID : CVE-2021-25500**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=11	H-SAM-EXYN-221121/710
Siemens					
apogee_modular_building_controller					
Access of	09-Nov-21	5	A vulnerability has been	https://cert-	H-SIE-APOG-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Using Incompatible Type ('Type Confusion')			identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**	portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	221121/711
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf,	H-SIE-APOG-221121/712

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
			(PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**	https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf,	H-SIE-APOG-221121/713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**	https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf,	H-SIE-APOG-221121/714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**	https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/	H-SIE-APOG-221121/715

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
			Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**	ssa-114589.pdf	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**		
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/717

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
			versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**		
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/718

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
			(All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**		
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “USER” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "PWD/XPWD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validate the length of the "MKD/XMKD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/722

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
			conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**		
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**		
apogee_modular_equiment_controller					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/724

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
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/727
Improper Restriction of Operations	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC	https://cert-portal.siemens.com/productcert/pdf/	H-SIE-APOG-221121/728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			(PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**	ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Restriction of Operations within the Bounds of a Memory	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-	H-SIE-APOG-221121/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**	portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-	H-SIE-APOG-221121/730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**	114589.pdf	
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/731

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
			Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**		
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/732

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
			Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "USER" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "PWD/XPWD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “MKD/XMKD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**		
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked.	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**		
apogee_pxc_compact					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**		
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008)	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31881		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/741
Improper Restriction	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC	https://cert-portal.sieme	H-SIE-APOG-221121/742

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
of Operations within the Bounds of a Memory Buffer			(PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**	ns.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf,	H-SIE-APOG-221121/743

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
			(PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**	https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-	H-SIE-APOG-221121/744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**	portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-	H-SIE-APOG-221121/745

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
			versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "USER" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**	114589.pdf	
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/746

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
			Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "PWD/XPWD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "MKD/XMKD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**		
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**		
apogee_pxc_modular					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/752

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 IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**		
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/754

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
			conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/755
Out-of-	09-Nov-21	7.5	A vulnerability has been	https://cert-	H-SIE-APOG-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**	portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	221121/756
Buffer Access with	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC	https://cert-portal.sieme	H-SIE-APOG-221121/757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Length Value			(PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**	ns.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf,	H-SIE-APOG-221121/758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “USER” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**	https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/prod	H-SIE-APOG-221121/759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “PWD/XPWD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**	uctcert/pdf/ssa-114589.pdf	
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "MKD/XMKD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**		
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-APOG-221121/762

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
			< V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**		
climatix_pol909					
Missing Encryption of Sensitive Data	09-Nov-21	5.8	A vulnerability has been identified in Climatix POL909 (AWM module) (All versions < V11.34). The web server of affected devices transmits data without TLS encryption. This could allow an unauthenticated remote attacker in a man-in-the-middle position to read sensitive data, such as administrator credentials, or modify data in transit. **CVE ID : CVE-2021-40366**	https://cert-portal.siemens.com/productcert/pdf/ssa-703715.pdf	H-SIE-CLIM-221121/763
talon_tc_compact					
Access of Resource Using	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All	https://cert-portal.siemens.com/prod	H-SIE-TALO-221121/764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incompatible Type ('Type Confusion')			versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**	uctcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.sieme	H-SIE-TALO-221121/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**	ns.com/productcert/pdf/ssa-114589.pdf	
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.sieme	H-SIE-TALO-221121/766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**	ns.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.sieme	H-SIE-TALO-221121/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**	ns.com/productcert/pdf/ssa-114589.pdf	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**		
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the “Hostname” DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**		
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**		
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "USER" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server does not properly validate the length of the “PWD/XPWD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “MKD/XMKD” command,	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015)	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/775

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
			CVE ID : CVE-2021-31889		
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017)	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31890		
talon_tc_modular					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/777
Improper Validation of Specified	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All	https://cert-portal.siemens.com/prod	H-SIE-TALO-221121/778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Quantity in Input			versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**	uctcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Validation of Specified	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All	https://cert-portal.siemens.com/prod	H-SIE-TALO-221121/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Quantity in Input			versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**	uctcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All	https://cert-portal.siemens.com/prod	H-SIE-TALO-221121/780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**	uctcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Restriction of Operations within the Bounds of a Memory	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-	H-SIE-TALO-221121/781

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
Buffer			versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**	portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/	H-SIE-TALO-221121/782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**	ssa-114589.pdf	
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/783

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
			Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**		
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**		
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "USER" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “PWD/XPWD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "MKD/XMKD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**		
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	H-SIE-TALO-221121/789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**		
Operating System					
airangel					
hsmx-app-1000_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-21	3.5	Airangel HSMX Gateway devices through 5.2.04 is vulnerable to stored Cross Site Scripting. XSS Payload is placed in the name column of the updates table using database access. **CVE ID : CVE-2021-40517**	N/A	O-AIR-HSMX-221121/790
Use of Hard-coded Credentials	10-Nov-21	6.4	Airangel HSMX Gateway devices through 5.2.04 have Hard-coded Database Credentials. **CVE ID : CVE-2021-40519**	N/A	O-AIR-HSMX-221121/791
N/A	10-Nov-21	10	Airangel HSMX Gateway devices through 5.2.04 allow Remote Code Execution. **CVE ID : CVE-2021-40521**	N/A	O-AIR-HSMX-221121/792
hsmx-app-100_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-21	3.5	Airangel HSMX Gateway devices through 5.2.04 is vulnerable to stored Cross Site Scripting. XSS Payload is placed in the name column of the updates table using database access. **CVE ID : CVE-2021-40517**	N/A	O-AIR-HSMX-221121/793

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
Use of Hard-coded Credentials	10-Nov-21	6.4	Airangel HSMX Gateway devices through 5.2.04 have Hard-coded Database Credentials. **CVE ID : CVE-2021-40519**	N/A	O-AIR-HSMX-221121/794
N/A	10-Nov-21	10	Airangel HSMX Gateway devices through 5.2.04 allow Remote Code Execution. **CVE ID : CVE-2021-40521**	N/A	O-AIR-HSMX-221121/795
hsmx-app-20000_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-21	3.5	Airangel HSMX Gateway devices through 5.2.04 is vulnerable to stored Cross Site Scripting. XSS Payload is placed in the name column of the updates table using database access. **CVE ID : CVE-2021-40517**	N/A	O-AIR-HSMX-221121/796
Use of Hard-coded Credentials	10-Nov-21	6.4	Airangel HSMX Gateway devices through 5.2.04 have Hard-coded Database Credentials. **CVE ID : CVE-2021-40519**	N/A	O-AIR-HSMX-221121/797
N/A	10-Nov-21	10	Airangel HSMX Gateway devices through 5.2.04 allow Remote Code Execution. **CVE ID : CVE-2021-40521**	N/A	O-AIR-HSMX-221121/798
hsmx-app-25_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site	10-Nov-21	3.5	Airangel HSMX Gateway devices through 5.2.04 is vulnerable to stored Cross Site Scripting. XSS Payload is placed in the name column of the updates table using database access.	N/A	O-AIR-HSMX-221121/799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			**CVE ID : CVE-2021-40517**		
Use of Hard-coded Credentials	10-Nov-21	6.4	Airangel HSMX Gateway devices through 5.2.04 have Hard-coded Database Credentials. **CVE ID : CVE-2021-40519**	N/A	O-AIR-HSMX-221121/800
N/A	10-Nov-21	10	Airangel HSMX Gateway devices through 5.2.04 allow Remote Code Execution. **CVE ID : CVE-2021-40521**	N/A	O-AIR-HSMX-221121/801
hsmx-app-5000_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-21	3.5	Airangel HSMX Gateway devices through 5.2.04 is vulnerable to stored Cross Site Scripting. XSS Payload is placed in the name column of the updates table using database access. **CVE ID : CVE-2021-40517**	N/A	O-AIR-HSMX-221121/802
Use of Hard-coded Credentials	10-Nov-21	6.4	Airangel HSMX Gateway devices through 5.2.04 have Hard-coded Database Credentials. **CVE ID : CVE-2021-40519**	N/A	O-AIR-HSMX-221121/803
N/A	10-Nov-21	10	Airangel HSMX Gateway devices through 5.2.04 allow Remote Code Execution. **CVE ID : CVE-2021-40521**	N/A	O-AIR-HSMX-221121/804
Apple					
iphone_os					
N/A	09-Nov-21	5	In JetBrains YouTrack Mobile before 2021.2, the client-side cache on iOS could contain sensitive	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-	O-APP-IPHO-221121/805

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
			information. **CVE ID : CVE-2021-43187**	security-bulletin-q3-2021/	
N/A	09-Nov-21	5	JetBrains YouTrack Mobile before 2021.2, is missing the security screen on Android and iOS. **CVE ID : CVE-2021-43191**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	O-APP-IPHO-221121/806
N/A	09-Nov-21	5	In JetBrains YouTrack Mobile before 2021.2, iOS URL scheme hijacking is possible. **CVE ID : CVE-2021-43192**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	O-APP-IPHO-221121/807
Beckhoff					
tf6100_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Nov-21	8.5	TwinCAT OPC UA Server in TF6100 and TS6100 in product versions before 4.3.48.0 or with TcOpcUaServer versions below 3.2.0.194 are prone to a relative path traversal that allow administrators to create or delete any files on the system. **CVE ID : CVE-2021-34594**	https://cert.vde.com/en/advisories/VDE-2021-051/	O-BEC-TF61-221121/808
ts6100_firmware					
Improper Limitation of a Pathname to a Restricted	04-Nov-21	8.5	TwinCAT OPC UA Server in TF6100 and TS6100 in product versions before 4.3.48.0 or with TcOpcUaServer versions	https://cert.vde.com/en/advisories/VDE-2021-051/	O-BEC-TS61-221121/809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			below 3.2.0.194 are prone to a relative path traversal that allow administrators to create or delete any files on the system. **CVE ID : CVE-2021-34594**		
beeline					
smart_box_firmware					
Cross-Site Request Forgery (CSRF)	10-Nov-21	6.8	Beeline Smart box 2.0.38 is vulnerable to Cross Site Request Forgery (CSRF) via mgt_end_user.htm. **CVE ID : CVE-2021-41426**	https://tula.beeline.ru/customers/pomosh/home/domashnij-internet/nastrojki-s-routerom/beelinesmartbox/	O-BEE-SMAR-221121/810
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-21	4.3	Beeline Smart Box 2.0.38 is vulnerable to Cross Site Scripting (XSS) via the choose_mac parameter to setup.cgi. **CVE ID : CVE-2021-41427**	https://tula.beeline.ru/customers/pomosh/home/domashnij-internet/nastrojki-s-routerom/beelinesmartbox/	O-BEE-SMAR-221121/811
Cisco					
catalyst_pon_switch_cgp-ont-1p_firmware					
Use of Hard-coded Credentials	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-	O-CIS-CATA-221121/812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34795**	multivulns-CE3DSYGr	
Improper Input Validation	04-Nov-21	5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40112**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	O-CIS-CATA-221121/813
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-	O-CIS-CATA-221121/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40113**	multivulns-CE3DSYGr	
catalyst_pon_switch_cgp-ont-4pvc_firmware					
Use of Hard-coded Credentials	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34795**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	O-CIS-CATA-221121/815
Improper Input Validation	04-Nov-21	5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	O-CIS-CATA-221121/816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40112**	sco-sa-catpon-multivulns-CE3DSYGr	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40113**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	O-CIS-CATA-221121/817
catalyst_pon_switch_cgp-ont-4pv_firmware					
Use of Hard-coded Credentials	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical	https://tools.cisco.com/security/center/content/	O-CIS-CATA-221121/818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34795**	CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	
Improper Input Validation	04-Nov-21	5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40112**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	O-CIS-CATA-221121/819
Improper Neutralization of Special Elements	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical	https://tools.cisco.com/security/center/content/	O-CIS-CATA-221121/820

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
used in a Command ('Command Injection')			Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40113**	CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	
catalyst_pon_switch_cgp-ont-4p_firmware					
Use of Hard-coded Credentials	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34795**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	O-CIS-CATA-221121/821
Improper Input	04-Nov-21	5	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/s	O-CIS-CATA-221121/822

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
Validation			interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40112**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40113**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	O-CIS-CATA-221121/823
catalyst_pon_switch_cgp-ont-4tvcw_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34795**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	O-CIS-CATA-221121/824
Improper Input Validation	04-Nov-21	5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40112**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	O-CIS-CATA-221121/825

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
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Nov-21	7.5	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40113**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr	O-CIS-CATA-221121/826
ios_xr					
Improper Input Validation	04-Nov-21	9	A vulnerability in the web-based management interface of certain Cisco Small Business RV Series Routers could allow an authenticated, remote attacker with administrative privileges to inject arbitrary commands into the underlying operating system and execute them using root-level privileges. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to a specific	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-cmdinjection-Z5cWFdK	O-CIS-IOS_-221121/827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			field in the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as a user with root-level privileges. **CVE ID : CVE-2021-40120**		
sf200-24fp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF20-221121/828

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
			resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf200-24p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF20-221121/829
sf200-24_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart	https://tools.cisco.com/security/center/content/	O-CIS-SF20-221121/830

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
			Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	
sf200-48p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF20-221121/831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf200-48_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF20-221121/832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf200e-24p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF20-221121/833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf200e-24_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF20-221121/834
sf200e-48p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small	https://tools.cisco.com/security/cent	O-CIS-SF20-221121/835

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
			Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	er/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	
sf200e-48_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF20-221121/836

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
			attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf300-08_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF30-221121/837

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
			could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf300-24mp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF30-221121/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf300-24pp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF30-221121/839
sf300-24p_firmware					
Improper Input	04-Nov-21	5	A vulnerability in the web-based management	https://tools.cisco.com/s	O-CIS-SF30-221121/840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	
sf300-24_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF30-221121/841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf300-48pp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF30-221121/842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf300-48p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF30-221121/843

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
			for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf300-48_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF30-221121/844
sf302-08mpp_firmware					
Improper	04-Nov-21	5	A vulnerability in the web-	https://tools	O-CIS-SF30-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	221121/845
sf302-08mp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-	O-CIS-SF30-221121/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	xMyFFkt8	
sf302-08pp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF30-221121/847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf302-08p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF30-221121/848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf302-08_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF30-221121/849
sf500-24mp_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF50-221121/850
sf500-24p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-	O-CIS-SF50-221121/851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	web-dos-xMyFFkt8	
sf500-24_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF50-221121/852

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
			This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf500-48mp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF50-221121/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sf500-48p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF50-221121/854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf500-48_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SF50-221121/855
sg200-08p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	O-CIS-SG20-221121/856

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
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg200-08_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG20-221121/857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg200-10fp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG20-221121/858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg200-18_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG20-221121/859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg200-26fp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG20-221121/860
sg200-26p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	O-CIS-SG20-221121/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg200-26_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG20-221121/862

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
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg200-50fp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG20-221121/863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg200-50p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG20-221121/864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg200-50_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG20-221121/865
sg300-10mpp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	O-CIS-SG30-221121/866

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
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg300-10mp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG30-221121/867

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
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg300-10pp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG30-221121/868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg300-10p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG30-221121/869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-10_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG30-221121/870
sg300-20_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	O-CIS-SG30-221121/871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg300-28mp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG30-221121/872

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
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg300-28pp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG30-221121/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg300-28p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG30-221121/874

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
sg300-28sfp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG30-221121/875
sg300-28_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	O-CIS-SG30-221121/876

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
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg300-52mp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG30-221121/877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg300-52p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG30-221121/878

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
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg300-52_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG30-221121/879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-sfp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG30-221121/880
sg500-28mpp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	O-CIS-SG50-221121/881

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
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg500-28p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG50-221121/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg500-28_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG50-221121/883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg500-52mp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG50-221121/884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg500-52p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG50-221121/885
sg500-52_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	O-CIS-SG50-221121/886

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
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg500x-24mpp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG50-221121/887

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
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg500x-24p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG50-221121/888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg500x-24_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG50-221121/889

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
sg500x-48mpp_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG50-221121/890
sg500x-48p_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-	O-CIS-SG50-221121/891

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
			Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**	switches-web-dos-xMyFFkt8	
sg500x-48_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG50-221121/892

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
			service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
sg500xg-8f8t_firmware					
Improper Input Validation	04-Nov-21	5	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8	O-CIS-SG50-221121/893

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
			exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition. **CVE ID : CVE-2021-40127**		
Fedoraproject					
fedora					
Use After Free	02-Nov-21	6.8	Use after free in Garbage Collection in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37977**	https://crbug.com/1252878, https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop.html	O-FED-FEDO-221121/894
Out-of-bounds Write	02-Nov-21	6.8	Heap buffer overflow in Blink in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37978**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop.html, https://crbug.com/1236318	O-FED-FEDO-221121/895
Out-of-bounds Write	02-Nov-21	6.8	heap buffer overflow in WebRTC in Google Chrome prior to 94.0.4606.81 allowed a remote attacker who convinced a user to	https://chromereleases.googleblog.com/2021/10/stable-	O-FED-FEDO-221121/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			browse to a malicious website to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37979**	channel-update-for-desktop.html, https://crbug.com/1247260	
N/A	02-Nov-21	4.3	Inappropriate implementation in Sandbox in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially bypass site isolation via Windows. **CVE ID : CVE-2021-37980**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop.html, https://crbug.com/1254631	O-FED-FEDO-221121/897
Fortinet					
fortios					
Improper Certificate Validation	02-Nov-21	4.3	An improper validation of certificate with host mismatch [CWE-297] vulnerability in FortiOS versions 6.4.6 and below may allow the connection to a malicious LDAP server via options in GUI, leading to disclosure of sensitive information, such as AD credentials. **CVE ID : CVE-2021-41019**	https://fortiguard.com/advisory/FG-IR-21-074	O-FOR-FORT-221121/898
Google					
android					
N/A	09-Nov-21	5	In JetBrains YouTrack Mobile before 2021.2, task hijacking on Android is	https://blog.jetbrains.com/blog/202	O-GOO-ANDR-221121/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			possible. **CVE ID : CVE-2021-43190**	1/11/08/jetbrains-security-bulletin-q3-2021/	
N/A	09-Nov-21	5	JetBrains YouTrack Mobile before 2021.2, is missing the security screen on Android and iOS. **CVE ID : CVE-2021-43191**	https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/	O-GOO-ANDR-221121/900
Improper Input Validation	05-Nov-21	2.1	A missing input validation in HDCP LDFW prior to SMR Nov-2021 Release 1 allows attackers to overwrite TZASC allowing TEE compromise. **CVE ID : CVE-2021-25500**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=11	O-GOO-ANDR-221121/901
Incorrect Authorization	05-Nov-21	2.1	An improper access control vulnerability in SCloudBnRReceiver in SecTelephonyProvider prior to SMR Nov-2021 Release 1 allows untrusted application to call some protected providers. **CVE ID : CVE-2021-25501**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=11	O-GOO-ANDR-221121/902
Cleartext Storage of Sensitive Information	05-Nov-21	2.1	A vulnerability of storing sensitive information insecurely in Property Settings prior to SMR Nov-2021 Release 1 allows attackers to read ESN value without priviledge. **CVE ID : CVE-2021-25502**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=11	O-GOO-ANDR-221121/903
Improper	05-Nov-21	4.6	Improper input validation	https://secu	O-GOO-ANDR-

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
Input Validation			vulnerability in HDCP prior to SMR Nov-2021 Release 1 allows attackers to arbitrary code execution. **CVE ID : CVE-2021-25503**	rity.samsungmobile.com/securityUpdate.smsb?year=2021&month=11	221121/904
HP					
futuresmart_3					
N/A	03-Nov-21	2.1	Certain HP LaserJet, HP LaserJet Managed, HP PageWide, and HP PageWide Managed printers may be vulnerable to potential information disclosure. **CVE ID : CVE-2021-39237**	https://support.hp.com/us-en/document/ish_5000124-5000148-16	O-HP-FUTU-221121/905
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Nov-21	7.5	Certain HP Enterprise LaserJet, HP LaserJet Managed, HP Enterprise PageWide, HP PageWide Managed products may be vulnerable to potential buffer overflow. **CVE ID : CVE-2021-39238**	https://support.hp.com/us-en/document/ish_5000383-5000409-16	O-HP-FUTU-221121/906
futuresmart_4					
N/A	03-Nov-21	2.1	Certain HP LaserJet, HP LaserJet Managed, HP PageWide, and HP PageWide Managed printers may be vulnerable to potential information disclosure. **CVE ID : CVE-2021-39237**	https://support.hp.com/us-en/document/ish_5000124-5000148-16	O-HP-FUTU-221121/907
Buffer Copy without Checking Size of Input ('Classic	03-Nov-21	7.5	Certain HP Enterprise LaserJet, HP LaserJet Managed, HP Enterprise PageWide, HP PageWide Managed products may be	https://support.hp.com/us-en/document/ish_50003	O-HP-FUTU-221121/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			vulnerable to potential buffer overflow. **CVE ID : CVE-2021-39238**	83-5000409-16	
futuresmart_5					
N/A	03-Nov-21	2.1	Certain HP LaserJet, HP LaserJet Managed, HP PageWide, and HP PageWide Managed printers may be vulnerable to potential information disclosure. **CVE ID : CVE-2021-39237**	https://support.hp.com/us-en/document/ish_5000124-5000148-16	O-HP-FUTU-221121/909
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Nov-21	7.5	Certain HP Enterprise LaserJet, HP LaserJet Managed, HP Enterprise PageWide, HP PageWide Managed products may be vulnerable to potential buffer overflow. **CVE ID : CVE-2021-39238**	https://support.hp.com/us-en/document/ish_5000383-5000409-16	O-HP-FUTU-221121/910
laserjet_pro_j8h60a_firmware					
Uncontrolled Resource Consumption	01-Nov-21	7.8	Potential security vulnerabilities have been discovered on a certain HP LaserJet Pro printer that may allow a Denial of Service on the device. **CVE ID : CVE-2021-3704**	https://support.hp.com/us-en/document/ish_4411563-4411589-16/hpsbpi03741	O-HP-LASE-221121/911
Incorrect Authorization	01-Nov-21	10	Potential security vulnerabilities have been discovered on a certain HP LaserJet Pro printer that may allow an unauthorized user to reconfigure, reset the device. **CVE ID : CVE-2021-3705**	https://support.hp.com/us-en/document/ish_4411563-4411589-16/hpsbpi0	O-HP-LASE-221121/912

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
				3741	
laserjet_pro_j8h61a_firmware					
Uncontrolled Resource Consumption	01-Nov-21	7.8	Potential security vulnerabilities have been discovered on a certain HP LaserJet Pro printer that may allow a Denial of Service on the device. **CVE ID : CVE-2021-3704**	https://support.hp.com/us-en/document/ish_4411563-4411589-16/hpsbpi03741	O-HP-LASE-221121/913
Incorrect Authorization	01-Nov-21	10	Potential security vulnerabilities have been discovered on a certain HP LaserJet Pro printer that may allow an unauthorized user to reconfigure, reset the device. **CVE ID : CVE-2021-3705**	https://support.hp.com/us-en/document/ish_4411563-4411589-16/hpsbpi03741	O-HP-LASE-221121/914
hpe					
proliant_dl20_gen10_server_firmware					
N/A	01-Nov-21	7.2	A potential local bypass of security restrictions vulnerability has been identified in HPE ProLiant DL20 Gen10, HPE ProLiant ML30 Gen10, and HPE ProLiant MicroServer Gen10 Plus server's system ROMs prior to version 2.52. The vulnerability could be locally exploited to cause disclosure of sensitive information, denial of service (DoS), and/or compromise system integrity.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04197en_us	O-HPE-PROL-221121/915

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
			CVE ID : CVE-2021-29213		
proliant_microserver_gen10_plus_firmware					
N/A	01-Nov-21	7.2	A potential local bypass of security restrictions vulnerability has been identified in HPE ProLiant DL20 Gen10, HPE ProLiant ML30 Gen10, and HPE ProLiant MicroServer Gen10 Plus server's system ROMs prior to version 2.52. The vulnerability could be locally exploited to cause disclosure of sensitive information, denial of service (DoS), and/or compromise system integrity. **CVE ID : CVE-2021-29213**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04197en_us	O-HPE-PROL-221121/916
proliant_ml30_gen10_server_firmware					
N/A	01-Nov-21	7.2	A potential local bypass of security restrictions vulnerability has been identified in HPE ProLiant DL20 Gen10, HPE ProLiant ML30 Gen10, and HPE ProLiant MicroServer Gen10 Plus server's system ROMs prior to version 2.52. The vulnerability could be locally exploited to cause disclosure of sensitive information, denial of service (DoS), and/or compromise system integrity. **CVE ID : CVE-2021-29213**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04197en_us	O-HPE-PROL-221121/917
IBM					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
aix					
XML Injection (aka Blind XPath Injection)	02-Nov-21	6.4	IBM InfoSphere Information Server 11.7 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 211402. **CVE ID : CVE-2021-38948**	https://www.ibm.com/support/pages/node/6509632, https://exchange.xforce.ibmcloud.com/vulnerabilities/211402	O-IBM-AIX-221121/918
Improper Certificate Validation	02-Nov-21	5	IBM InfoSphere Data Flow Designer Engine (IBM InfoSphere Information Server 11.7) component has improper validation of the REST API server certificate. IBM X-Force ID: 201301. **CVE ID : CVE-2021-29737**	https://exchange.xforce.ibmcloud.com/vulnerabilities/201301, https://www.ibm.com/support/pages/node/6509086	O-IBM-AIX-221121/919
Server-Side Request Forgery (SSRF)	02-Nov-21	5.5	IBM InfoSphere Data Flow Designer (IBM InfoSphere Information Server 11.7) 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. IBM X-Force ID: 201302. **CVE ID : CVE-2021-29738**	https://exchange.xforce.ibmcloud.com/vulnerabilities/201302, https://www.ibm.com/support/pages/node/6509084	O-IBM-AIX-221121/920
Improper	02-Nov-21	3.5	IBM InfoSphere Information	https://ww	O-IBM-AIX-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			Server 11.7 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. **CVE ID : CVE-2021-29771**	w.ibm.com/support/pages/node/6509614, https://exchange.xforce.ibmcloud.com/vulnerabilities/202773	221121/921
Cross-Site Request Forgery (CSRF)	02-Nov-21	6.8	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 207123. **CVE ID : CVE-2021-29888**	https://exchange.xforce.ibmcloud.com/vulnerabilities/207123, https://www.ibm.com/support/pages/node/6509618	O-IBM-AIX-221121/922
Linux					
linux_kernel					
XML Injection (aka Blind XPath Injection)	02-Nov-21	6.4	IBM InfoSphere Information Server 11.7 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 211402. **CVE ID : CVE-2021-38948**	https://www.ibm.com/support/pages/node/6509632, https://exchange.xforce.ibmcloud.com/vulnerabilities/211402	O-LIN-LINU-221121/923
Improper Input	02-Nov-21	7.5	An issue was discovered in net/tipc/crypto.c in the Linux kernel before 5.14.16.	https://github.com/torvalds/linux/c	O-LIN-LINU-221121/924

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
Validation			The Transparent Inter-Process Communication (TIPC) functionality allows remote attackers to exploit insufficient validation of user-supplied sizes for the MSG_CRYPTO message type. **CVE ID : CVE-2021-43267**	ommit/fa40d9734a57bcbfa79a280189799f76c88f7bb0, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.14.16	
Out-of-bounds Read	04-Nov-21	2.1	An issue was discovered in the Linux kernel before 5.14.15. There is an array-index-out-of-bounds flaw in the detach_capi_ctr function in drivers/isdn/capi/kcapi.c. **CVE ID : CVE-2021-43389**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=1f3e2e97c003f80c4b087092b225c8787ff91e4d, https://bugzilla.redhat.com/show_bug.cgi?id=2013180	O-LIN-LINU-221121/925
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-21	3.5	IBM Security Guardium 10.5, 10.6, 11.0, 11.1, 11.2, and 11.3 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. **CVE ID : CVE-2021-29735**	https://www.ibm.com/support/pages/node/6514007, https://exchange.xforce.ibmcloud.com/vulnerabilities/201239	O-LIN-LINU-221121/926

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
Improper Certificate Validation	02-Nov-21	5	IBM InfoSphere Data Flow Designer Engine (IBM InfoSphere Information Server 11.7) component has improper validation of the REST API server certificate. IBM X-Force ID: 201301. **CVE ID : CVE-2021-29737**	https://exchange.xforce.ibmcloud.com/vulnerabilities/201301, https://www.ibm.com/support/pages/node/6509086	O-LIN-LINU-221121/927
Server-Side Request Forgery (SSRF)	02-Nov-21	5.5	IBM InfoSphere Data Flow Designer (IBM InfoSphere Information Server 11.7) 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. IBM X-Force ID: 201302. **CVE ID : CVE-2021-29738**	https://exchange.xforce.ibmcloud.com/vulnerabilities/201302, https://www.ibm.com/support/pages/node/6509084	O-LIN-LINU-221121/928
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-21	3.5	IBM InfoSphere Information Server 11.7 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. **CVE ID : CVE-2021-29771**	https://www.ibm.com/support/pages/node/6509614, https://exchange.xforce.ibmcloud.com/vulnerabilities/202773	O-LIN-LINU-221121/929
Cross-Site Request	02-Nov-21	6.8	IBM InfoSphere Information Server 11.7 is vulnerable to	https://exchange.xforce.i	O-LIN-LINU-221121/930

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
Forgery (CSRF)			cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 207123. **CVE ID : CVE-2021-29888**	bmcloud.com/vulnerabilities/207123, https://www.ibm.com/support/pages/node/6509618	
meross					
mss550x_firmware					
Missing Encryption of Sensitive Data	05-Nov-21	4.3	Meross Smart Wi-Fi 2 Way Wall Switch (MSS550X), on its 3.1.3 version and before, creates an open Wi-Fi Access Point without the required security measures in its initial setup. This could allow a remote attacker to obtain the Wi-Fi SSID as well as the password configured by the user from Meross app via Http/JSON plain request. **CVE ID : CVE-2021-3774**	https://www.incibe-cert.es/en/early-warning/security-advisories/meross-mss550x-missing-encryption-sensitive-data	O-MER-MSS5-221121/931
Microsoft					
windows					
N/A	03-Nov-21	7.8	Possible system denial of service in case of arbitrary changing Firefox browser parameters. An attacker could change specific Firefox browser parameters file in a certain way and then reboot the system to make the system unbootable. **CVE ID : CVE-2021-35053**	N/A	O-MIC-WIND-221121/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Nov-21	4.3	Inappropriate implementation in Sandbox in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially bypass site isolation via Windows. **CVE ID : CVE-2021-37980**	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop.html, https://crbug.com/1254631	O-MIC-WIND-221121/933
N/A	03-Nov-21	4.3	When delegating navigations to the operating system, Firefox would accept the `mk` scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. *This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 92, Thunderbird < 91.1, Thunderbird < 78.14, Firefox ESR < 78.14, and Firefox ESR < 91.1. **CVE ID : CVE-2021-38492**	https://www.mozilla.org/security/advisories/mfsa2021-41/, https://www.mozilla.org/security/advisories/mfsa2021-40/, https://www.mozilla.org/security/advisories/mfsa2021-42/, https://www.mozilla.org/security/advisories/mfsa2021-38/	O-MIC-WIND-221121/934
XML Injection (aka Blind XPath Injection)	02-Nov-21	6.4	IBM InfoSphere Information Server 11.7 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive	https://www.ibm.com/support/pages/node/6509632, https://exchange.xforce.ibmcloud.co	O-MIC-WIND-221121/935

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
			information or consume memory resources. IBM X-Force ID: 211402. **CVE ID : CVE-2021-38948**	m/vulnerabilities/211402	
Improper Privilege Management	02-Nov-21	4.6	A improper privilege management in Fortinet FortiSIEM Windows Agent version 4.1.4 and below allows attacker to execute privileged code or commands via powershell scripts **CVE ID : CVE-2021-41022**	https://fortiguard.com/advisory/FG-IR-21-176	O-MIC-WIND-221121/936
Cleartext Storage of Sensitive Information	02-Nov-21	2.1	A unprotected storage of credentials in Fortinet FortiSIEM Windows Agent version 4.1.4 and below allows an authenticated user to disclosure agent password due to plaintext credential storage in log files **CVE ID : CVE-2021-41023**	https://fortiguard.com/advisory/FG-IR-21-175	O-MIC-WIND-221121/937
Improper Certificate Validation	02-Nov-21	5	IBM InfoSphere Data Flow Designer Engine (IBM InfoSphere Information Server 11.7) component has improper validation of the REST API server certificate. IBM X-Force ID: 201301. **CVE ID : CVE-2021-29737**	https://exchange.xforce.ibmcloud.com/vulnerabilities/201301, https://www.ibm.com/support/pages/node/6509086	O-MIC-WIND-221121/938
Server-Side Request Forgery (SSRF)	02-Nov-21	5.5	IBM InfoSphere Data Flow Designer (IBM InfoSphere Information Server 11.7) is vulnerable to server-side request forgery (SSRF). This	https://exchange.xforce.ibmcloud.com/vulnerabilities/20130	O-MIC-WIND-221121/939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 201302. **CVE ID : CVE-2021-29738**	2, https://www.ibm.com/support/pages/node/6509084	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-21	3.5	IBM InfoSphere Information Server 11.7 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. **CVE ID : CVE-2021-29771**	https://www.ibm.com/support/pages/node/6509614, https://exchange.xforce.ibmcloud.com/vulnerabilities/202773	O-MIC-WIND-221121/940
Cross-Site Request Forgery (CSRF)	02-Nov-21	6.8	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 207123. **CVE ID : CVE-2021-29888**	https://exchange.xforce.ibmcloud.com/vulnerabilities/207123, https://www.ibm.com/support/pages/node/6509618	O-MIC-WIND-221121/941
windows_10					
Improper Privilege Management	10-Nov-21	4.6	Windows Desktop Bridge Elevation of Privilege Vulnerability **CVE ID : CVE-2021-36957**	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-221121/942

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
				visory/CVE-2021-36957	
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-41371. **CVE ID : CVE-2021-38631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38631	O-MIC-WIND-221121/943
N/A	10-Nov-21	4.3	Remote Desktop Protocol Client Information Disclosure Vulnerability **CVE ID : CVE-2021-38665**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38665	O-MIC-WIND-221121/944
N/A	10-Nov-21	6.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2021-38666**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38666	O-MIC-WIND-221121/945
N/A	10-Nov-21	4.3	Microsoft Edge (Chrome based) Spoofing on IE Mode **CVE ID : CVE-2021-41351**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41351	O-MIC-WIND-221121/946
N/A	10-Nov-21	5	Windows Denial of Service Vulnerability **CVE ID : CVE-2021-41356**	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221121/947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2021-41356	
Improper Privilege Management	10-Nov-21	4.6	Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41366**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41366	O-MIC-WIND-221121/948
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41370, CVE-2021-42283. **CVE ID : CVE-2021-41367**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41367	O-MIC-WIND-221121/949
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-42283. **CVE ID : CVE-2021-41370**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41370	O-MIC-WIND-221121/950
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-38631. **CVE ID : CVE-2021-41371**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41371	O-MIC-WIND-221121/951
Improper Privilege Management	10-Nov-21	4.6	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41377**	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221121/952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				US/security-guidance/advisory/CVE-2021-41377	
N/A	10-Nov-21	6.5	Windows NTFS Remote Code Execution Vulnerability **CVE ID : CVE-2021-41378**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41378	O-MIC-WIND-221121/953
Improper Privilege Management	10-Nov-21	4.6	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41379**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41379	O-MIC-WIND-221121/954
N/A	10-Nov-21	2.1	Windows Hyper-V Discrete Device Assignment (DDA) Denial of Service Vulnerability **CVE ID : CVE-2021-42274**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42274	O-MIC-WIND-221121/955
N/A	10-Nov-21	6.5	Microsoft COM for Windows Remote Code Execution Vulnerability **CVE ID : CVE-2021-42275**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42275	O-MIC-WIND-221121/956
N/A	10-Nov-21	6.8	Microsoft Windows Media Foundation Remote Code Execution Vulnerability	https://portal.msrc.microsoft.com/e	O-MIC-WIND-221121/957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-42276	n-US/security-guidance/advisory/CVE-2021-42276	
Improper Privilege Management	10-Nov-21	4.6	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42277**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42277	O-MIC-WIND-221121/958
Out-of-bounds Write	10-Nov-21	5.1	Chakra Scripting Engine Memory Corruption Vulnerability **CVE ID : CVE-2021-42279**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42279	O-MIC-WIND-221121/959
Improper Privilege Management	10-Nov-21	4.6	Windows Feedback Hub Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42280**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42280	O-MIC-WIND-221121/960
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-41370. **CVE ID : CVE-2021-42283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42283	O-MIC-WIND-221121/961
Uncontrolled Resource	10-Nov-21	7.1	Windows Hyper-V Denial of Service Vulnerability	https://portal.msrc.micr	O-MIC-WIND-221121/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			**CVE ID : CVE-2021-42284**	osoft.com/en-US/security-guidance/advisory/CVE-2021-42284	
Improper Privilege Management	10-Nov-21	7.2	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42285	O-MIC-WIND-221121/963
Improper Privilege Management	10-Nov-21	4.6	Windows Core Shell SI Host Extension Framework for Composable Shell Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42286**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42286	O-MIC-WIND-221121/964
N/A	10-Nov-21	7.7	Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability **CVE ID : CVE-2021-26443**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26443	O-MIC-WIND-221121/965
windows_11					
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-41371. **CVE ID : CVE-2021-38631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38631	O-MIC-WIND-221121/966

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
N/A	10-Nov-21	4.3	Remote Desktop Protocol Client Information Disclosure Vulnerability **CVE ID : CVE-2021-38665**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38665	O-MIC-WIND-221121/967
N/A	10-Nov-21	6.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2021-38666**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38666	O-MIC-WIND-221121/968
N/A	10-Nov-21	4.3	Microsoft Edge (Chrome based) Spoofing on IE Mode **CVE ID : CVE-2021-41351**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41351	O-MIC-WIND-221121/969
N/A	10-Nov-21	5	Windows Denial of Service Vulnerability **CVE ID : CVE-2021-41356**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41356	O-MIC-WIND-221121/970
Improper Privilege Management	10-Nov-21	4.6	Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41366**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-221121/971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-41366	
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41370, CVE-2021-42283. **CVE ID : CVE-2021-41367**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41367	O-MIC-WIND-221121/972
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-42283. **CVE ID : CVE-2021-41370**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41370	O-MIC-WIND-221121/973
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-38631. **CVE ID : CVE-2021-41371**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41371	O-MIC-WIND-221121/974
Improper Privilege Management	10-Nov-21	4.6	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41377**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41377	O-MIC-WIND-221121/975
N/A	10-Nov-21	6.5	Windows NTFS Remote Code Execution Vulnerability **CVE ID : CVE-2021-41378**	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-221121/976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visory/CVE-2021-41378	
Improper Privilege Management	10-Nov-21	4.6	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41379**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41379	O-MIC-WIND-221121/977
N/A	10-Nov-21	2.1	Windows Hyper-V Discrete Device Assignment (DDA) Denial of Service Vulnerability **CVE ID : CVE-2021-42274**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42274	O-MIC-WIND-221121/978
N/A	10-Nov-21	6.5	Microsoft COM for Windows Remote Code Execution Vulnerability **CVE ID : CVE-2021-42275**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42275	O-MIC-WIND-221121/979
N/A	10-Nov-21	6.8	Microsoft Windows Media Foundation Remote Code Execution Vulnerability **CVE ID : CVE-2021-42276**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42276	O-MIC-WIND-221121/980
Improper Privilege Management	10-Nov-21	4.6	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42277**	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221121/981

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
				guidance/advisory/CVE-2021-42277	
Out-of-bounds Write	10-Nov-21	5.1	Chakra Scripting Engine Memory Corruption Vulnerability **CVE ID : CVE-2021-42279**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42279	O-MIC-WIND-221121/982
Improper Privilege Management	10-Nov-21	4.6	Windows Feedback Hub Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42280**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42280	O-MIC-WIND-221121/983
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-41370. **CVE ID : CVE-2021-42283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42283	O-MIC-WIND-221121/984
Uncontrolled Resource Consumption	10-Nov-21	7.1	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2021-42284**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42284	O-MIC-WIND-221121/985
Improper Privilege Management	10-Nov-21	7.2	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42285**	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221121/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				US/security-guidance/advisory/CVE-2021-42285	
N/A	10-Nov-21	7.7	Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability **CVE ID : CVE-2021-26443**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26443	O-MIC-WIND-221121/987
windows_7					
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-41371. **CVE ID : CVE-2021-38631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38631	O-MIC-WIND-221121/988
N/A	10-Nov-21	4.3	Remote Desktop Protocol Client Information Disclosure Vulnerability **CVE ID : CVE-2021-38665**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38665	O-MIC-WIND-221121/989
N/A	10-Nov-21	6.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2021-38666**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38666	O-MIC-WIND-221121/990
Improper Privilege	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is	https://portal.msrc.micr	O-MIC-WIND-221121/991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			unique from CVE-2021-41370, CVE-2021-42283. **CVE ID : CVE-2021-41367**	osoft.com/en-US/security-guidance/advisory/CVE-2021-41367	
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-42283. **CVE ID : CVE-2021-41370**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41370	O-MIC-WIND-221121/992
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-38631. **CVE ID : CVE-2021-41371**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41371	O-MIC-WIND-221121/993
Improper Privilege Management	10-Nov-21	4.6	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41377**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41377	O-MIC-WIND-221121/994
Improper Privilege Management	10-Nov-21	4.6	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41379**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41379	O-MIC-WIND-221121/995
N/A	10-Nov-21	6.5	Microsoft COM for Windows	https://port	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability **CVE ID : CVE-2021-42275**	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42275	221121/996
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-41370. **CVE ID : CVE-2021-42283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42283	O-MIC-WIND-221121/997
Improper Privilege Management	10-Nov-21	7.2	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42285	O-MIC-WIND-221121/998
windows_8.1					
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-41371. **CVE ID : CVE-2021-38631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38631	O-MIC-WIND-221121/999
N/A	10-Nov-21	4.3	Remote Desktop Protocol Client Information Disclosure Vulnerability **CVE ID : CVE-2021-38665**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-221121/1000

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
				2021-38665	
N/A	10-Nov-21	6.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2021-38666**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38666	O-MIC-WIND-221121/1001
Improper Privilege Management	10-Nov-21	4.6	Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41366**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41366	O-MIC-WIND-221121/1002
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41370, CVE-2021-42283. **CVE ID : CVE-2021-41367**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41367	O-MIC-WIND-221121/1003
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-42283. **CVE ID : CVE-2021-41370**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41370	O-MIC-WIND-221121/1004
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-38631. **CVE ID : CVE-2021-41371**	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-221121/1005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visory/CVE-2021-41371	
Improper Privilege Management	10-Nov-21	4.6	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41377**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41377	O-MIC-WIND-221121/1006
Improper Privilege Management	10-Nov-21	4.6	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41379**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41379	O-MIC-WIND-221121/1007
N/A	10-Nov-21	6.5	Microsoft COM for Windows Remote Code Execution Vulnerability **CVE ID : CVE-2021-42275**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42275	O-MIC-WIND-221121/1008
Uncontrolled Resource Consumption	10-Nov-21	7.1	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2021-42284**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42284	O-MIC-WIND-221121/1009
Improper Privilege Management	10-Nov-21	7.2	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42285**	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221121/1010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2021-42285	
windows_rt_8.1					
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-41371. **CVE ID : CVE-2021-38631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38631	O-MIC-WIND-221121/1011
N/A	10-Nov-21	4.3	Remote Desktop Protocol Client Information Disclosure Vulnerability **CVE ID : CVE-2021-38665**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38665	O-MIC-WIND-221121/1012
N/A	10-Nov-21	6.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2021-38666**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38666	O-MIC-WIND-221121/1013
Improper Privilege Management	10-Nov-21	4.6	Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41366**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41366	O-MIC-WIND-221121/1014
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-	https://portal.microsoft.com/e	O-MIC-WIND-221121/1015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			41370, CVE-2021-42283. **CVE ID : CVE-2021-41367**	n-US/security-guidance/advisory/CVE-2021-41367	
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-42283. **CVE ID : CVE-2021-41370**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41370	O-MIC-WIND-221121/1016
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-38631. **CVE ID : CVE-2021-41371**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41371	O-MIC-WIND-221121/1017
Improper Privilege Management	10-Nov-21	4.6	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41377**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41377	O-MIC-WIND-221121/1018
Improper Privilege Management	10-Nov-21	4.6	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41379**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41379	O-MIC-WIND-221121/1019
N/A	10-Nov-21	6.5	Microsoft COM for Windows Remote Code Execution	https://portal.msrc.micr	O-MIC-WIND-221121/1020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability **CVE ID : CVE-2021-42275**	osoft.com/en-US/security-guidance/advisory/CVE-2021-42275	
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-41370. **CVE ID : CVE-2021-42283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42283	O-MIC-WIND-221121/1021
Improper Privilege Management	10-Nov-21	7.2	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42285	O-MIC-WIND-221121/1022
windows_server					
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42287, CVE-2021-42291. **CVE ID : CVE-2021-42282**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42282	O-MIC-WIND-221121/1023
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-41370. **CVE ID : CVE-2021-42283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42283	O-MIC-WIND-221121/1024

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
Uncontrolled Resource Consumption	10-Nov-21	7.1	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2021-42284**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42284	O-MIC-WIND-221121/1025
Improper Privilege Management	10-Nov-21	7.2	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42285	O-MIC-WIND-221121/1026
Improper Privilege Management	10-Nov-21	4.6	Windows Core Shell SI Host Extension Framework for Composable Shell Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42286**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42286	O-MIC-WIND-221121/1027
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42282, CVE-2021-42291. **CVE ID : CVE-2021-42287**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42287	O-MIC-WIND-221121/1028
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42282, CVE-2021-42287. **CVE ID : CVE-2021-42291**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-221121/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-42291	
windows_server_2008					
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-41371. **CVE ID : CVE-2021-38631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38631	O-MIC-WIND-221121/1030
N/A	10-Nov-21	4.3	Remote Desktop Protocol Client Information Disclosure Vulnerability **CVE ID : CVE-2021-38665**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38665	O-MIC-WIND-221121/1031
N/A	10-Nov-21	6.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2021-38666**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38666	O-MIC-WIND-221121/1032
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41370, CVE-2021-42283. **CVE ID : CVE-2021-41367**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41367	O-MIC-WIND-221121/1033
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-42283.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221121/1034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-41370	guidance/advisory/CVE-2021-41370	
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-38631. **CVE ID : CVE-2021-41371**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41371	O-MIC-WIND-221121/1035
Improper Privilege Management	10-Nov-21	4.6	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41377**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41377	O-MIC-WIND-221121/1036
Improper Privilege Management	10-Nov-21	4.6	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41379**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41379	O-MIC-WIND-221121/1037
N/A	10-Nov-21	6.5	Microsoft COM for Windows Remote Code Execution Vulnerability **CVE ID : CVE-2021-42275**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42275	O-MIC-WIND-221121/1038
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221121/1039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-42282, CVE-2021-42287, CVE-2021-42291. **CVE ID : CVE-2021-42278**	US/security-guidance/advisory/CVE-2021-42278	
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42287, CVE-2021-42291. **CVE ID : CVE-2021-42282**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42282	O-MIC-WIND-221121/1040
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-41370. **CVE ID : CVE-2021-42283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42283	O-MIC-WIND-221121/1041
Improper Privilege Management	10-Nov-21	7.2	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42285	O-MIC-WIND-221121/1042
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42282, CVE-2021-42291. **CVE ID : CVE-2021-42287**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42287	O-MIC-WIND-221121/1043
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This	https://portal.msrc.microsoft.com/e	O-MIC-WIND-221121/1044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2021-42278, CVE-2021-42282, CVE-2021-42287. **CVE ID : CVE-2021-42291**	n-US/security-guidance/advisory/CVE-2021-42291	
windows_server_2012					
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-41371. **CVE ID : CVE-2021-38631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38631	O-MIC-WIND-221121/1045
N/A	10-Nov-21	4.3	Remote Desktop Protocol Client Information Disclosure Vulnerability **CVE ID : CVE-2021-38665**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38665	O-MIC-WIND-221121/1046
N/A	10-Nov-21	6.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2021-38666**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38666	O-MIC-WIND-221121/1047
Improper Privilege Management	10-Nov-21	4.6	Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41366**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41366	O-MIC-WIND-221121/1048
Improper	10-Nov-21	4.6	NTFS Elevation of Privilege	https://port	O-MIC-WIND-

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
Privilege Management			Vulnerability This CVE ID is unique from CVE-2021-41370, CVE-2021-42283. **CVE ID : CVE-2021-41367**	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41367	221121/1049
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-42283. **CVE ID : CVE-2021-41370**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41370	O-MIC-WIND-221121/1050
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-38631. **CVE ID : CVE-2021-41371**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41371	O-MIC-WIND-221121/1051
Improper Privilege Management	10-Nov-21	4.6	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41377**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41377	O-MIC-WIND-221121/1052
Improper Privilege Management	10-Nov-21	4.6	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41379**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41379	O-MIC-WIND-221121/1053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Nov-21	6.5	Microsoft COM for Windows Remote Code Execution Vulnerability **CVE ID : CVE-2021-42275**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42275	O-MIC-WIND-221121/1054
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42282, CVE-2021-42287, CVE-2021-42291. **CVE ID : CVE-2021-42278**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42278	O-MIC-WIND-221121/1055
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42287, CVE-2021-42291. **CVE ID : CVE-2021-42282**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42282	O-MIC-WIND-221121/1056
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-41370. **CVE ID : CVE-2021-42283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42283	O-MIC-WIND-221121/1057
Uncontrolled Resource Consumption	10-Nov-21	7.1	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2021-42284**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-221121/1058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-42284	
Improper Privilege Management	10-Nov-21	7.2	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42285	O-MIC-WIND-221121/1059
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42282, CVE-2021-42291. **CVE ID : CVE-2021-42287**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42287	O-MIC-WIND-221121/1060
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42282, CVE-2021-42287. **CVE ID : CVE-2021-42291**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42291	O-MIC-WIND-221121/1061
windows_server_2016					
Improper Privilege Management	10-Nov-21	4.6	Windows Desktop Bridge Elevation of Privilege Vulnerability **CVE ID : CVE-2021-36957**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36957	O-MIC-WIND-221121/1062
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-41371.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221121/1063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-38631	guidance/advisory/CVE-2021-38631	
N/A	10-Nov-21	4.3	Remote Desktop Protocol Client Information Disclosure Vulnerability **CVE ID : CVE-2021-38665**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38665	O-MIC-WIND-221121/1064
N/A	10-Nov-21	6.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2021-38666**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38666	O-MIC-WIND-221121/1065
N/A	10-Nov-21	5	Windows Denial of Service Vulnerability **CVE ID : CVE-2021-41356**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41356	O-MIC-WIND-221121/1066
Improper Privilege Management	10-Nov-21	4.6	Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41366**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41366	O-MIC-WIND-221121/1067
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41370, CVE-2021-42283.	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221121/1068

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
			CVE ID : CVE-2021-41367	US/security-guidance/advisory/CVE-2021-41367	
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-42283. **CVE ID : CVE-2021-41370**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41370	O-MIC-WIND-221121/1069
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-38631. **CVE ID : CVE-2021-41371**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41371	O-MIC-WIND-221121/1070
Improper Privilege Management	10-Nov-21	4.6	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41377**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41377	O-MIC-WIND-221121/1071
N/A	10-Nov-21	6.5	Windows NTFS Remote Code Execution Vulnerability **CVE ID : CVE-2021-41378**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41378	O-MIC-WIND-221121/1072
Improper Privilege Management	10-Nov-21	4.6	Windows Installer Elevation of Privilege Vulnerability	https://portal.msrc.microsoft.com/e	O-MIC-WIND-221121/1073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-41379	n-US/security-guidance/advisory/CVE-2021-41379	
N/A	10-Nov-21	2.1	Windows Hyper-V Discrete Device Assignment (DDA) Denial of Service Vulnerability **CVE ID : CVE-2021-42274**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42274	O-MIC-WIND-221121/1074
N/A	10-Nov-21	6.5	Microsoft COM for Windows Remote Code Execution Vulnerability **CVE ID : CVE-2021-42275**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42275	O-MIC-WIND-221121/1075
N/A	10-Nov-21	6.8	Microsoft Windows Media Foundation Remote Code Execution Vulnerability **CVE ID : CVE-2021-42276**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42276	O-MIC-WIND-221121/1076
Improper Privilege Management	10-Nov-21	4.6	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42277**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42277	O-MIC-WIND-221121/1077
Improper Privilege	10-Nov-21	6.5	Active Directory Domain Services Elevation of	https://portal.msrc.micr	O-MIC-WIND-221121/1078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Privilege Vulnerability This CVE ID is unique from CVE-2021-42282, CVE-2021-42287, CVE-2021-42291. **CVE ID : CVE-2021-42278**	osoft.com/en-US/security-guidance/advisory/CVE-2021-42278	
Out-of-bounds Write	10-Nov-21	5.1	Chakra Scripting Engine Memory Corruption Vulnerability **CVE ID : CVE-2021-42279**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42279	O-MIC-WIND-221121/1079
Improper Privilege Management	10-Nov-21	4.6	Windows Feedback Hub Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42280**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42280	O-MIC-WIND-221121/1080
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42287, CVE-2021-42291. **CVE ID : CVE-2021-42282**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42282	O-MIC-WIND-221121/1081
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-41370. **CVE ID : CVE-2021-42283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42283	O-MIC-WIND-221121/1082
Uncontrolled	10-Nov-21	7.1	Windows Hyper-V Denial of	https://port	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			Service Vulnerability **CVE ID : CVE-2021-42284**	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42284	221121/1083
Improper Privilege Management	10-Nov-21	7.2	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42285	O-MIC-WIND-221121/1084
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42282, CVE-2021-42291. **CVE ID : CVE-2021-42287**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42287	O-MIC-WIND-221121/1085
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42282, CVE-2021-42287. **CVE ID : CVE-2021-42291**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42291	O-MIC-WIND-221121/1086
N/A	10-Nov-21	7.7	Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability **CVE ID : CVE-2021-26443**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26443	O-MIC-WIND-221121/1087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
windows_server_2019					
Improper Privilege Management	10-Nov-21	4.6	Windows Desktop Bridge Elevation of Privilege Vulnerability **CVE ID : CVE-2021-36957**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36957	O-MIC-WIND-221121/1088
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-41371. **CVE ID : CVE-2021-38631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38631	O-MIC-WIND-221121/1089
N/A	10-Nov-21	4.3	Remote Desktop Protocol Client Information Disclosure Vulnerability **CVE ID : CVE-2021-38665**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38665	O-MIC-WIND-221121/1090
N/A	10-Nov-21	6.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2021-38666**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38666	O-MIC-WIND-221121/1091
N/A	10-Nov-21	4.3	Microsoft Edge (Chrome based) Spoofing on IE Mode **CVE ID : CVE-2021-41351**	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-221121/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visory/CVE-2021-41351	
N/A	10-Nov-21	5	Windows Denial of Service Vulnerability **CVE ID : CVE-2021-41356**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41356	O-MIC-WIND-221121/1093
Improper Privilege Management	10-Nov-21	4.6	Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41366**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41366	O-MIC-WIND-221121/1094
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41370, CVE-2021-42283. **CVE ID : CVE-2021-41367**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41367	O-MIC-WIND-221121/1095
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-42283. **CVE ID : CVE-2021-41370**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41370	O-MIC-WIND-221121/1096
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-38631.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221121/1097

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
			CVE ID : CVE-2021-41371	guidance/advisory/CVE-2021-41371	
Improper Privilege Management	10-Nov-21	4.6	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41377**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41377	O-MIC-WIND-221121/1098
N/A	10-Nov-21	6.5	Windows NTFS Remote Code Execution Vulnerability **CVE ID : CVE-2021-41378**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41378	O-MIC-WIND-221121/1099
Improper Privilege Management	10-Nov-21	4.6	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41379**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41379	O-MIC-WIND-221121/1100
N/A	10-Nov-21	2.1	Windows Hyper-V Discrete Device Assignment (DDA) Denial of Service Vulnerability **CVE ID : CVE-2021-42274**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42274	O-MIC-WIND-221121/1101
N/A	10-Nov-21	6.5	Microsoft COM for Windows Remote Code Execution Vulnerability **CVE ID : CVE-2021-42275**	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221121/1102

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
				US/security-guidance/advisory/CVE-2021-42275	
N/A	10-Nov-21	6.8	Microsoft Windows Media Foundation Remote Code Execution Vulnerability **CVE ID : CVE-2021-42276**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42276	O-MIC-WIND-221121/1103
Improper Privilege Management	10-Nov-21	4.6	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42277**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42277	O-MIC-WIND-221121/1104
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42282, CVE-2021-42287, CVE-2021-42291. **CVE ID : CVE-2021-42278**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42278	O-MIC-WIND-221121/1105
Out-of-bounds Write	10-Nov-21	5.1	Chakra Scripting Engine Memory Corruption Vulnerability **CVE ID : CVE-2021-42279**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42279	O-MIC-WIND-221121/1106
Improper Privilege Management	10-Nov-21	4.6	Windows Feedback Hub Elevation of Privilege Vulnerability	https://portal.msrc.microsoft.com/e	O-MIC-WIND-221121/1107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-42280	n-US/security-guidance/advisory/CVE-2021-42280	
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42287, CVE-2021-42291. **CVE ID : CVE-2021-42282**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42282	O-MIC-WIND-221121/1108
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-41370. **CVE ID : CVE-2021-42283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42283	O-MIC-WIND-221121/1109
Uncontrolled Resource Consumption	10-Nov-21	7.1	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2021-42284**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42284	O-MIC-WIND-221121/1110
Improper Privilege Management	10-Nov-21	7.2	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42285	O-MIC-WIND-221121/1111
Improper Privilege	10-Nov-21	6.5	Active Directory Domain Services Elevation of	https://portal.micr	O-MIC-WIND-221121/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42282, CVE-2021-42291. **CVE ID : CVE-2021-42287**	osoft.com/en-US/security-guidance/advisory/CVE-2021-42287	
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42282, CVE-2021-42287. **CVE ID : CVE-2021-42291**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42291	O-MIC-WIND-221121/1113
N/A	10-Nov-21	7.7	Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability **CVE ID : CVE-2021-26443**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26443	O-MIC-WIND-221121/1114
windows_server_2022					
Improper Privilege Management	10-Nov-21	4.6	Windows Desktop Bridge Elevation of Privilege Vulnerability **CVE ID : CVE-2021-36957**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36957	O-MIC-WIND-221121/1115
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-41371. **CVE ID : CVE-2021-38631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38631	O-MIC-WIND-221121/1116

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
N/A	10-Nov-21	4.3	Remote Desktop Protocol Client Information Disclosure Vulnerability **CVE ID : CVE-2021-38665**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38665	O-MIC-WIND-221121/1117
N/A	10-Nov-21	6.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2021-38666**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38666	O-MIC-WIND-221121/1118
N/A	10-Nov-21	5	Windows Denial of Service Vulnerability **CVE ID : CVE-2021-41356**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41356	O-MIC-WIND-221121/1119
Improper Privilege Management	10-Nov-21	4.6	Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41366**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41366	O-MIC-WIND-221121/1120
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41370, CVE-2021-42283. **CVE ID : CVE-2021-41367**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-221121/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-41367	
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-42283. **CVE ID : CVE-2021-41370**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41370	O-MIC-WIND-221121/1122
N/A	10-Nov-21	2.1	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-38631. **CVE ID : CVE-2021-41371**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41371	O-MIC-WIND-221121/1123
Improper Privilege Management	10-Nov-21	4.6	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41377**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41377	O-MIC-WIND-221121/1124
N/A	10-Nov-21	6.5	Windows NTFS Remote Code Execution Vulnerability **CVE ID : CVE-2021-41378**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41378	O-MIC-WIND-221121/1125
Improper Privilege Management	10-Nov-21	4.6	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-41379**	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-221121/1126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visory/CVE-2021-41379	
N/A	10-Nov-21	2.1	Windows Hyper-V Discrete Device Assignment (DDA) Denial of Service Vulnerability **CVE ID : CVE-2021-42274**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42274	O-MIC-WIND-221121/1127
N/A	10-Nov-21	6.5	Microsoft COM for Windows Remote Code Execution Vulnerability **CVE ID : CVE-2021-42275**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42275	O-MIC-WIND-221121/1128
N/A	10-Nov-21	6.8	Microsoft Windows Media Foundation Remote Code Execution Vulnerability **CVE ID : CVE-2021-42276**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42276	O-MIC-WIND-221121/1129
Improper Privilege Management	10-Nov-21	4.6	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42277**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42277	O-MIC-WIND-221121/1130
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42282, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221121/1131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			42287, CVE-2021-42291. **CVE ID : CVE-2021-42278**	guidance/advisory/CVE-2021-42278	
Out-of-bounds Write	10-Nov-21	5.1	Chakra Scripting Engine Memory Corruption Vulnerability **CVE ID : CVE-2021-42279**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42279	O-MIC-WIND-221121/1132
Improper Privilege Management	10-Nov-21	4.6	Windows Feedback Hub Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42280**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42280	O-MIC-WIND-221121/1133
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42287, CVE-2021-42291. **CVE ID : CVE-2021-42282**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42282	O-MIC-WIND-221121/1134
Improper Privilege Management	10-Nov-21	4.6	NTFS Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-41367, CVE-2021-41370. **CVE ID : CVE-2021-42283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42283	O-MIC-WIND-221121/1135
Uncontrolled Resource Consumption	10-Nov-21	7.1	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2021-42284**	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221121/1136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				US/security-guidance/advisory/CVE-2021-42284	
Improper Privilege Management	10-Nov-21	7.2	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2021-42285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42285	O-MIC-WIND-221121/1137
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42282, CVE-2021-42291. **CVE ID : CVE-2021-42287**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42287	O-MIC-WIND-221121/1138
Improper Privilege Management	10-Nov-21	6.5	Active Directory Domain Services Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-42278, CVE-2021-42282, CVE-2021-42287. **CVE ID : CVE-2021-42291**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42291	O-MIC-WIND-221121/1139
N/A	10-Nov-21	7.7	Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability **CVE ID : CVE-2021-26443**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26443	O-MIC-WIND-221121/1140
Realtek					
rtl8195am_firmware					

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Nov-21	7.5	A buffer overflow was discovered on Realtek RTL8195AM devices before 2.0.10. It exists in the client code when processing a malformed IE length of HT capability information in the Beacon and Association response frame. **CVE ID : CVE-2021-43573**	https://realtek.com	O-REA-RTL8-221121/1141
Redhat					
enterprise_linux					
Out-of-bounds Read	04-Nov-21	2.1	An issue was discovered in the Linux kernel before 5.14.15. There is an array-index-out-of-bounds flaw in the detach_capi_ctr function in drivers/isdn/capi/kcapi.c. **CVE ID : CVE-2021-43389**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=1f3e2e97c003f80c4b087092b225c8787ff91e4d, https://bugzilla.redhat.com/show_bug.cgi?id=2013180	O-RED-ENTE-221121/1142
Siemens					
apogee_modular_building_controller_firmware					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/prod	O-SIE-APOG-221121/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**	uctcert/pdf/ssa-114589.pdf	
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1144

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
			Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**		
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1146

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
			Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1147

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
			(All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			< V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**		
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the “Hostname” DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**		
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**		
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "USER" command, leading	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "PWD/XPWD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "MKD/XMKD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018)	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31888		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1154
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-	O-SIE-APOG-221121/1155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**	044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
apogee_modular_equiment_controller_firmware					
Access of Resource Using Incompatible	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC	https://cert-portal.siemens.com/productcert/pdf/	O-SIE-APOG-221121/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type ('Type Confusion')			(PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**	ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/prod	O-SIE-APOG-221121/1157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**	uctcert/pdf/ssa-114589.pdf	
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/prod	O-SIE-APOG-221121/1158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**	uctcert/pdf/ssa-114589.pdf	
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/prod	O-SIE-APOG-221121/1159

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
			versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**	uctcert/pdf/ssa-114589.pdf	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1160

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
			versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**		
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**		
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			< V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**		
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "USER" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validate the length of the "PWD/XPWD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "MKD/XMKD" command, leading to stack-based	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
apogee_pxc_compact_firmware					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1169
Improper Validation of Specified Quantity in	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC	https://cert-portal.siemens.com/productcert/pdf/	O-SIE-APOG-221121/1170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input			(PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**	ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Validation of Specified Quantity in	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC	https://cert-portal.siemens.com/productcert/pdf/	O-SIE-APOG-221121/1171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input			(PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**	ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC	https://cert-portal.siemens.com/productcert/pdf/	O-SIE-APOG-221121/1172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**	ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.sieme	O-SIE-APOG-221121/1173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**	ns.com/productcert/pdf/ssa-114589.pdf	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-	O-SIE-APOG-221121/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**	114589.pdf	
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1175

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
			versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**		
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**		
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “USER” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "PWD/XPWD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(BACnet) (All versions). FTP server does not properly validate the length of the "MKD/XMKD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**		
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**		
apogee_pxc_modular_firmware					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004)	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31344		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006)	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31345		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007)	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31346		
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1185
Improper Restriction of	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All	https://cert-portal.siemens.com/prod	O-SIE-APOG-221121/1186

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
Operations within the Bounds of a Memory Buffer			versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**	uctcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Restriction of Operations within the Bounds of a	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf,	O-SIE-APOG-221121/1187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			(PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**	https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/	O-SIE-APOG-221121/1188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**	ssa-114589.pdf	
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-	O-SIE-APOG-221121/1189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**	114589.pdf	
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “USER” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "PWD/XPWD" command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			< V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “MKD/XMKD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**		
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-APOG-221121/1194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**		
climatix_pol909_firmware					
Missing Encryption of Sensitive Data	09-Nov-21	5.8	A vulnerability has been identified in Climatix POL909 (AWM module) (All versions < V11.34). The web server of affected devices transmits data without TLS encryption. This could allow an unauthenticated remote attacker in a man-in-the-middle position to read sensitive data, such as administrator credentials, or modify data in transit. **CVE ID : CVE-2021-40366**	https://cert-portal.siemens.com/productcert/pdf/ssa-703715.pdf	O-SIE-CLIM-221121/1195
talon_tc_compact_firmware					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1198

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
			versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**		
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			< V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**		
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**		
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**		
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the "USER" command, leading to stack-based buffer overflows. This may result in Denial-of-Service	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1204

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
			conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “PWD/XPWD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016)	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31887		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “MKD/XMKD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1206
Integer Underflow	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC	https://cert-portal.sieme	O-SIE-TALO-221121/1207

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
(Wrap or Wraparound)			(PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**	ns.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Handling of Inconsistent Structural Elements	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.sieme	O-SIE-TALO-221121/1208

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
			(PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**	ns.com/productcert/pdf/ssa-114589.pdf	
talon_tc_modular_firmware					
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-	O-SIE-TALO-221121/1209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004) **CVE ID : CVE-2021-31344**	portal.siemens.com/productcert/pdf/ssa-114589.pdf	
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006) **CVE ID : CVE-2021-31345**		
Improper Validation of Specified Quantity in Input	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1211

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
			Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007) **CVE ID : CVE-2021-31346**		
Out-of-bounds Read	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008) **CVE ID : CVE-2021-31881**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1213

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
			Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011) **CVE ID : CVE-2021-31882**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013) **CVE ID : CVE-2021-31883**		
Out-of-bounds Read	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014) **CVE ID : CVE-2021-31884**		
Buffer Access with Incorrect Length Value	09-Nov-21	5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1216

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
			Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009) **CVE ID : CVE-2021-31885**		
Out-of-bounds Write	09-Nov-21	7.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validate the length of the “USER” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010) **CVE ID : CVE-2021-31886**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “PWD/XPWD” command, leading to stack-based	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016) **CVE ID : CVE-2021-31887**		
Out-of-bounds Write	09-Nov-21	6.5	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “MKD/XMKD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Code Execution. (FSMD-2021-0018) **CVE ID : CVE-2021-31888**		
Integer Underflow (Wrap or Wraparound)	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015) **CVE ID : CVE-2021-31889**	https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	O-SIE-TALO-221121/1220
Improper Handling of Inconsistent	09-Nov-21	6.4	A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All	https://cert-portal.siemens.com/prod	O-SIE-TALO-221121/1221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Structural Elements			versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017) **CVE ID : CVE-2021-31890**	uctcert/pdf/ssa-044112.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-114589.pdf	