National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Oct 2021 Vol. 08 No. 19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
3xlogic					
infinias_access_control					
Exposure of Resource to Wrong Sphere	01-Oct-21	6.5	An issue was discovered in 3xLogic Infinias Access Control through 6.7.10708.0, affecting physical security. Users with login credentials assigned to a specific zone can send modified HTTP GET and POST requests, allowing them to view user data such as personal information and Prox card credentials. Also, an authorized user of one zone can send API requests to unlock electronic locks associated with zones they are unauthorized to have access to. They can also create new user logins for zones they were not authorized to access, including the root zone of the software. **CVE ID : CVE-2021-41847**	https://www.3xlogic.com/infinias-access-control	A-3XL-INFI-201021/1
accel-ppp					
accel-ppp					
Out-of-bounds Read	07-Oct-21	5	ACCEL-PPP 1.12.0 has an out-of-bounds read in triton_context_schedule if the client exits after	N/A	A-ACC-ACCE-201021/2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication. **CVE ID : CVE-2021-42054**		
accesspressthemes					
access_demo_importer					
Unrestricted Upload of File with Dangerous Type	11-Oct-21	6.5	Versions up to, and including, 1.0.6, of the Access Demo Importer WordPress plugin are vulnerable to arbitrary file uploads via the plugin_offline_installer AJAX action due to a missing capability check in the plugin_offline_installer_callback function found in the ~/inc/demo-functions.php. **CVE ID : CVE-2021-39317**	https://plugins.trac.wordpress.org/changeset/2602132/access-demo-importer/trunk/inc/demo-functions.php, https://plugins.trac.wordpress.org/changeset/2592642/access-demo-importer/trunk/inc/demo-functions.php	A-ACC-ACCE-201021/3
Adobe					
acrobat_dc					
Use After Free	07-Oct-21	6.8	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability when processing AcroForm listbox that could result in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability in that the	https://helpx.adobe.com/security/products/acrobat/apsb21-55.html	A-ADO-ACRO-201021/4

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			target must visit a malicious page or open a malicious file. **CVE ID : CVE-2021-40725**		
Use After Free	07-Oct-21	6.8	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability when processing AcroForm field that could result in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **CVE ID : CVE-2021-40726**	https://helpx.adobe.com/security/products/acrobat/apsb21-55.html	A-ADO-ACRO-201021/5
acrobat_reader_dc					
Use After Free	07-Oct-21	6.8	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability when processing AcroForm listbox that could result in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability in that the	https://helpx.adobe.com/security/products/acrobat/apsb21-55.html	A-ADO-ACRO-201021/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			target must visit a malicious page or open a malicious file. **CVE ID : CVE-2021-40725**		
Use After Free	07-Oct-21	6.8	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability when processing AcroForm field that could result in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **CVE ID : CVE-2021-40726**	https://helpx.adobe.com/security/products/acrobat/apsb21-55.html	A-ADO-ACRO-201021/7
xmp_toolkit_sdk					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Oct-21	6.8	XMP Toolkit SDK version 2020.1 (and earlier) is affected by a buffer overflow vulnerability potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a specially-crafted .cpp file. **CVE ID : CVE-2021-36051**	https://helpx.adobe.com/security/products/xmpcore/apsb21-65.html	A-ADO-XMP_-201021/8
afian					
filerun					

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 Input During Web Page Generation ('Cross-site Scripting')	05-Oct-21	4.3	Afian FileRun 2021.03.26 allows stored XSS via an HTTP X-Forwarded-For header that is mishandled when rendering Activity Logs. **CVE ID : CVE-2021-35503**	N/A	A-AFI-FILE-201021/9
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Oct-21	6.5	Afian FileRun 2021.03.26 allows Remote Code Execution (by administrators) via the Check Path value for the ffmpeg binary. **CVE ID : CVE-2021-35504**	N/A	A-AFI-FILE-201021/10
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Oct-21	6.5	Afian FileRun 2021.03.26 allows Remote Code Execution (by administrators) via the Check Path value for the magick binary. **CVE ID : CVE-2021-35505**	N/A	A-AFI-FILE-201021/11
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Oct-21	4.3	Afian FileRun 2021.03.26 allows XSS when an administrator encounters a crafted document during use of the HTML Editor for a preview or edit action. **CVE ID : CVE-2021-35506**	N/A	A-AFI-FILE-201021/12
Akamai					
enterprise_application_access					
Unquoted Search Path or Element	04-Oct-21	4.4	In Akamai EAA (Enterprise Application Access) Client before 2.3.1, 2.4.x before	https://www.akamai.com/products/enter	A-AKA-ENTE-201021/13

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.4.1, and 2.5.x before 2.5.3, an unquoted path may allow an attacker to hijack the flow of execution. **CVE ID : CVE-2021-40683**	prise-application-access, https://akamai.com/blog/news/eaa-client-escalation-of-privilege-vulnerability	
alfred-spotify-mini-player					
alfred_spotify_mini_player					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in callback.php in Spotify-for-Alfred 0.13.9 and below allows remote attackers to inject arbitrary web script or HTML via the error parameter. **CVE ID : CVE-2021-40927**	N/A	A-ALF-ALFR-201021/14
Alkacon					
opencms					
Improper Restriction of XML External Entity Reference	08-Oct-21	4	An XML external entity (XXE) vulnerability in Alkacon OpenCms 11.0, 11.0.1 and 11.0.2 allows remote authenticated users with edit privileges to exfiltrate files from the server's file system by uploading a crafted SVG document. **CVE ID : CVE-2021-3312**	N/A	A-ALK-OPEN-201021/15
Apache					
http_server					
NULL	05-Oct-21	5	While fuzzing the 2.4.49	https://httpd.	A-APA-HTTP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			httpd, a new null pointer dereference was detected during HTTP/2 request processing, allowing an external source to DoS the server. This requires a specially crafted request. The vulnerability was recently introduced in version 2.4.49. No exploit is known to the project. **CVE ID : CVE-2021-41524**	apache.org/security/vulnerabilities_24.html	201021/16
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Oct-21	4.3	A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue is known to be exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 was found to be incomplete, see CVE-2021-42013. **CVE ID : CVE-2021-41773**	https://httpd.apache.org/security/vulnerabilities_24.html, https://lists.apache.org/thread.html/r6abf5f2ba6f1aa8b1030f95367aaf17660c4e4c78cb2338aee18982f@%3Cusers.httpd.apache.org%3E	A-APA-HTTP-201021/17
Improper	07-Oct-21	7.5	It was found that the fix for	https://httpd.	A-APA-HTTP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			CVE-2021-41773 in Apache HTTP Server 2.4.50 was insufficient. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue only affects Apache 2.4.49 and Apache 2.4.50 and not earlier versions. **CVE ID : CVE-2021-42013**	apache.org/security/vulnerabilities_24.html, https://lists.apache.org/thread.html/r17a4c6ce9aff662efd9459e9d1850ab4a611cb23392fc68264c72cb3@%3Ccvs.httpd.apache.org%3E	201021/18
openoffice					
Improper Restriction of XML External Entity Reference	07-Oct-21	4.3	Apache OpenOffice has a dependency on expat software. Versions prior to 2.1.0 were subject to CVE-2013-0340 a "Billion Laughs" entity expansion denial of service attack and exploit via crafted XML files. ODF files consist of a set of XML files. All versions of Apache OpenOffice up to 4.1.10 are subject to this issue. expat in version 4.1.11 is patched. **CVE ID : CVE-2021-40439**	https://lists.apache.org/thread.html/rfb2c193360436e230b85547e85a41bea0916916f96c501f5b6fc4702%40%3Cusers.openoffice.apache.org%3E, https://lists.apache.org/thread.html/r41eca5f4f09e74436cbb05dec450fc2bef37b5d3e966aa7c	A-APA-OPEN-201021/19

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
				c5fada6d@%3Cannounce.apache.org%3E	
Improper Privilege Management	07-Oct-21	4.6	While working on Apache OpenOffice 4.1.8 a developer discovered that the DEB package did not install using root, but instead used a userid and groupid of 500. This both caused issues with desktop integration and could allow a crafted attack on files owned by that user or group if they exist. Users who installed the Apache OpenOffice 4.1.8 DEB packaging should upgrade to the latest version of Apache OpenOffice. **CVE ID : CVE-2021-28129**	https://lists.apache.org/thread.html/rc9090ab48b4699494b63b35cd6d7414c52d665ecae12add3cdc56c9b%40%3Cusers.openoffice.apache.org%3E, https://lists.apache.org/thread.html/r9e72234dd662280fa1a3cca6164d3470a1dbc0d8e53e48ba27f787ce@%3Cannounce.apache.org%3E	A-APA-OPEN-201021/20
archibus					
web_central					
Session Fixation	05-Oct-21	7.5	** UNSUPPORTED WHEN ASSIGNED ** In ARCHIBUS Web Central 21.3.3.815 (a version from 2014), the Web Application in /archibus/login.axvw assign a session token that could be already in use by another user. It was therefore possible to access the application through a user whose credentials were not known, without	N/A	A-ARC-WEB_-201021/21

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
			any attempt by the testers to modify the application logic. It is also possible to set the value of the session token, client-side, simply by making an unauthenticated GET Request to the Home Page and adding an arbitrary value to the JSESSIONID field. The application, following the login, does not assign a new token, continuing to keep the inserted one, as the identifier of the entire session. This is fixed in all recent versions, such as version 26. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Version 21.3 was officially de-supported by the end of 2020. **CVE ID : CVE-2021-41553**		
Incorrect Authorization	05-Oct-21	6.5	** UNSUPPORTED WHEN ASSIGNED ** ARCHIBUS Web Central 21.3.3.815 (a version from 2014) does not properly validate requests for access to data and functionality in these affected endpoints: /archibus/schema/ab-edit-users.axvw, /archibus/schema/ab-data-dictionary-table.axvw, /archibus/schema/ab-schema-add-field.axvw,	N/A	A-ARC-WEB_-201021/22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/archibus/schema/ab-core/views/process-navigator/ab-my-user-profile.axvw. By not verifying the permissions for access to resources, it allows a potential attacker to view pages that are not allowed. Specifically, it was found that any authenticated user can reach the administrative console for user management by directly requesting access to the page via URL. This allows a malicious user to modify all users' profiles, to elevate any privileges to administrative ones, or to create or delete any type of user. It is also possible to modify the emails of other users, through a misconfiguration of the username parameter, on the user profile page. This is fixed in all recent versions, such as version 26. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Version 21.3 was officially de-supported by the end of 2020. **CVE ID : CVE-2021-41554**		
Improper Neutralization of Input	05-Oct-21	4.3	** UNSUPPORTED WHEN ASSIGNED ** In ARCHIBUS Web Central 21.3.3.815 (a	N/A	A-ARC-WEB_-201021/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			version from 2014), XSS occurs in /archibus/dwr/call/plaincall/workflow.runWorkflowRule.dwr because the data received as input from clients is re-included within the HTTP response returned by the application without adequate validation. In this way, if HTML code or client-side executable code (e.g., Javascript) is entered as input, the expected execution flow could be altered. This is fixed in all recent versions, such as version 26. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Version 21.3 was officially de-supported by the end of 2020. **CVE ID : CVE-2021-41555**		
Artica					
integria_ims					
Unrestricted Upload of File with Dangerous Type	07-Oct-21	7.5	Integria IMS in its 5.0.92 version is vulnerable to a Remote Code Execution attack through file uploading. An unauthenticated attacker could abuse the AsyncUpload() function in order to exploit the vulnerability. **CVE ID : CVE-2021-3832**	https://www.incibe-cert.es/en/early-warning/security-advisories/integria-ims-remote-code-execution, https://integriaims.com/en	A-ART-INTE-201021/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/services/updates/	
Incorrect Authorization	07-Oct-21	7.5	Integria IMS login check uses a loose comparator ("==") to compare the MD5 hash of the password provided by the user and the MD5 hash stored in the database. An attacker with a specific formatted password could exploit this vulnerability in order to login in the system with different passwords. **CVE ID : CVE-2021-3833**	https://integriaims.com/en/services/updates/, https://www.incibe-cert.es/en/early-warning/security-advisories/integria-ims-incorrect-authorization	A-ART-INTE-201021/25
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-21	4.3	Integria IMS in its 5.0.92 version does not filter correctly some fields related to the login.php file. An attacker could exploit this vulnerability in order to perform a cross-site scripting attack (XSS). **CVE ID : CVE-2021-3834**	https://integriaims.com/en/services/updates/, https://www.incibe-cert.es/en/early-warning/security-advisories/integria-ims-vulnerable-cross-site-scripting-xss	A-ART-INTE-201021/26
aviatorscript_project					
aviatorscript					
Improper Neutralization of Special Elements in Output Used by a	02-Oct-21	7.5	AviatorScript through 5.2.7 allows code execution via an expression that is encoded with Byte Code Engineering Library (BCEL).	N/A	A-AVI-AVIA-201021/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Downstream Component ('Injection')			**CVE ID : CVE-2021-41862**		
awplife					
weather_effect					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-21	3.5	The Weather Effect WordPress plugin before 1.3.6 does not properly validate and escape some of its settings (like *_size_leaf, *_flakes_leaf, *_speed) which could lead to Stored Cross-Site Scripting issues **CVE ID : CVE-2021-24709**	N/A	A-AWP-WEAT-201021/28
ayecode					
geodirectory					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-21	3.5	The GeoDirectory Business Directory WordPress plugin before 2.1.1.3 was vulnerable to Authenticated Stored Cross-Site Scripting (XSS). **CVE ID : CVE-2021-24720**	https://plugins.trac.wordpress.org/changeset/2596452/geodirectory	A-AYE-GEOD-201021/29
biqs					
biqsdrive					
N/A	04-Oct-21	5	A local file inclusion (LFI) vulnerability exists in version BIQS IT Biqs-drive v1.83 and below when sending a specific payload as the file parameter to download/index.php. This allows the attacker to read arbitrary files from the server with the permissions of the	N/A	A-BIQ-BIQS-201021/30

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
			configured web-user. **CVE ID : CVE-2021-39433**		
bookingcore					
booking_core					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-21	3.5	Laravel Booking System Booking Core 2.0 is vulnerable to Cross Site Scripting (XSS). The Avatar upload in the My Profile section could be exploited to upload a malicious SVG file which contains Javascript. Now if another user/admin views the profile and clicks to view his avatar, an XSS will trigger. **CVE ID : CVE-2021-37330**	N/A	A-BOO-BOOK-201021/31
Improper Authentication	04-Oct-21	5	Laravel Booking System Booking Core 2.0 is vulnerable to Incorrect Access Control. On the Verifications page, after uploading an ID Card or Trade License and viewing it, ID Cards and Trade Licenses of other vendors/users can be viewed by changing the URL. **CVE ID : CVE-2021-37331**	N/A	A-BOO-BOOK-201021/32
Insufficient Session Expiration	04-Oct-21	7.5	Laravel Booking System Booking Core 2.0 is vulnerable to Session Management. A password change at sandbox.bookingcore.org/user/profile/change-	N/A	A-BOO-BOOK-201021/33

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			password does not invalidate a session that is opened in a different browser. **CVE ID : CVE-2021-37333**		
calibre-web_project					
calibre-web					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-21	3.5	In “Calibre-web” application, v0.6.0 to v0.6.12, are vulnerable to Stored XSS in “Metadata”. An attacker that has access to edit the metadata information, can inject JavaScript payload in the description field. When a victim tries to open the file, XSS will be triggered. **CVE ID : CVE-2021-25964**	https://github.com/janeczku/calibre-web/commit/32e27712f0f71fdec646add20cd78b4ce75acfce	A-CAL-CALI-201021/34
Canonical					
apport					
Exposure of Resource to Wrong Sphere	01-Oct-21	2.1	Function check_attachment_for_errors() in file data/general-hooks/ubuntu.py could be tricked into exposing private data via a constructed crash file. This issue affects: apport 2.14.1 versions prior to 2.14.1-0ubuntu3.29+esm8; 2.20.1 versions prior to 2.20.1-0ubuntu2.30+esm2; 2.20.9 versions prior to 2.20.9-0ubuntu7.26; 2.20.11 versions prior to 2.20.11-0ubuntu27.20; 2.20.11 versions prior to 2.20.11-	https://bugs.launchpad.net/ubuntu/+source/apport/+bug/1934308, https://ubuntu.com/security/notices/USN-5077-1, https://ubuntu.com/security/notices/USN-5077-2	A-CAN-APPO-201021/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0ubuntu65.3; **CVE ID : CVE-2021-3709**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Oct-21	4.7	An information disclosure via path traversal was discovered in apport/hookutils.py function read_file(). This issue affects: apport 2.14.1 versions prior to 2.14.1-0ubuntu3.29+esm8; 2.20.1 versions prior to 2.20.1-0ubuntu2.30+esm2; 2.20.9 versions prior to 2.20.9-0ubuntu7.26; 2.20.11 versions prior to 2.20.11-0ubuntu27.20; 2.20.11 versions prior to 2.20.11-0ubuntu65.3; **CVE ID : CVE-2021-3710**	https://ubuntu.com/security/notices/USN-5077-1, https://ubuntu.com/security/notices/USN-5077-2, https://bugs.launchpad.net/ubuntu/+source/apport/+bug/1933832	A-CAN-APPO-201021/36
multipass					
Improper Privilege Management	01-Oct-21	4.6	The Windows version of Multipass before 1.7.0 allowed any local process to connect to the localhost TCP control socket to perform mounts from the operating system to a guest, allowing for privilege escalation. **CVE ID : CVE-2021-3626**	https://github.com/canonical/multipass/pull/2150	A-CAN-MULT-201021/37
Incorrect Permission Assignment for Critical Resource	01-Oct-21	4.6	The MacOS version of Multipass, version 1.7.0, fixed in 1.7.2, accidentally installed the application directory with incorrect owner. **CVE ID : CVE-2021-3747**	https://github.com/canonical/multipass/issues/2261	A-CAN-MULT-201021/38
Cisco					

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
anyconnect_secure_mobility_client					
Time-of-check Time-of-use (TOCTOU) Race Condition	06-Oct-21	6.9	A vulnerability in the shared library loading mechanism of Cisco AnyConnect Secure Mobility Client for Linux and Mac OS could allow an authenticated, local attacker to perform a shared library hijacking attack on an affected device if the VPN Posture (HostScan) Module is installed on the AnyConnect client. This vulnerability is due to a race condition in the signature verification process for shared library files that are loaded on an affected device. An attacker could exploit this vulnerability by sending a series of crafted interprocess communication (IPC) messages to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected device with root privileges. To exploit this vulnerability, the attacker must have a valid account on the system. **CVE ID : CVE-2021-34788**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-lib-hija-cAFB7x4q	A-CIS-ANYC-201021/39
dna_center					
N/A	06-Oct-21	4	A vulnerability in the API endpoints for Cisco DNA	https://tools.cisco.com/sec	A-CIS-DNA_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Center could allow an authenticated, remote attacker to gain access to sensitive information that should be restricted. The attacker must have valid device credentials. This vulnerability is due to improper access controls on API endpoints. An attacker could exploit the vulnerability by sending a specific API request to an affected application. A successful exploit could allow the attacker to obtain sensitive information about other users who are configured with higher privileges on the application. **CVE ID : CVE-2021-34782**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-infodisc-KyC6YncS	201021/40
identity_services_engine					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	9.3	A vulnerability in the REST API of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to perform a command injection attack and elevate privileges to root. This vulnerability is due to insufficient input validation for specific API endpoints. An attacker in a man-in-the-middle position could exploit this vulnerability by intercepting and modifying specific internode communications from one	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-priv-esc-UwqPrBM3	A-CIS-IDEN-201021/41

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
			ISE persona to another ISE persona. A successful exploit could allow the attacker to run arbitrary commands with root privileges on the underlying operating system. To exploit this vulnerability, the attacker would need to decrypt HTTPS traffic between two ISE personas that are located on separate nodes. **CVE ID : CVE-2021-1594**		
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information. This vulnerability is due to improper enforcement of administrator privilege levels for low-value sensitive data. An attacker with read-only administrator access to the web-based management interface could exploit this vulnerability by browsing to the page that contains the sensitive data. A successful exploit could allow the attacker to collect sensitive information regarding the configuration of the system. **CVE ID : CVE-2021-34702**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-disc-pNXtLhdp	A-CIS-IDEN-201021/42
Improper	06-Oct-21	5.5	A vulnerability in the web-	https://tools.	A-CIS-IDEN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of XML External Entity Reference			based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to access sensitive information or conduct a server-side request forgery (SSRF) attack through an affected device. This vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by uploading a crafted XML file that contains references to external entities. A successful exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information, or cause the web application to perform arbitrary HTTP requests on behalf of the attacker. **CVE ID : CVE-2021-34706**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-V4VSjEsX	201021/43
intersight_virtual_appliance					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	9	A vulnerability in the web-based management interface of Cisco Intersight Virtual Appliance could allow an authenticated, remote attacker to perform a command injection attack on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsi2-command-inject-CGyC8y2R	A-CIS-INTE-201021/44

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation. An attacker could exploit this vulnerability by using the web-based management interface to execute a command using crafted input. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on an affected device. **CVE ID : CVE-2021-34748**		
orbital					
URL Redirection to Untrusted Site ('Open Redirect')	06-Oct-21	5.8	A vulnerability in the web-based management interface of Cisco Orbital could allow an unauthenticated, remote attacker to redirect users to a malicious webpage. This vulnerability is due to improper validation of URL paths in the web-based management interface. An attacker could exploit this vulnerability by persuading a user to click a crafted URL. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability, known as an open redirect attack, is used in phishing attacks to persuade users to visit malicious sites. **CVE ID : CVE-2021-34772**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-amp-redirect-rQ2Bu7dU	A-CIS-ORBI-201021/45
smart_software_manager_on-prem					

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 Privilege Management	06-Oct-21	6.5	A vulnerability in the web UI of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an authenticated, remote attacker to elevate privileges and create, read, update, or delete records and settings in multiple functions. This vulnerability is due to insufficient authorization of the System User and System Operator role capabilities. An attacker could exploit this vulnerability by directly accessing a web resource. A successful exploit could allow the attacker to create, read, update, or delete records and settings in multiple functions without the necessary permissions on the web UI. **CVE ID : CVE-2021-34766**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-priv-esc-5g35cdDJ	A-CIS-SMAR-201021/46
telepresence_collaboration_endpoint					
Incorrect Permission Assignment for Critical Resource	06-Oct-21	2.1	A vulnerability in the memory management of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an authenticated, local attacker to corrupt a shared memory segment, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient access controls	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tpce-rmos-mem-dos-rck56tT	A-CIS-TELE-201021/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a shared memory resource. An attacker could exploit this vulnerability by corrupting a shared memory segment on an affected device. A successful exploit could allow the attacker to cause the device to reload. The device will recover from the corruption upon reboot. **CVE ID : CVE-2021-34758**		
vision_dynamic_signage_director					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-21	4.3	A vulnerability in the web-based management interface of Cisco Vision Dynamic Signage Director could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface on an affected device. 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 of the interface 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.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cvdsd-xss-fvdj6HK	A-CIS-VISI-201021/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34742		
Cminds					
enhanced-tooltipglossary					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-21	3.5	The CM Tooltip Glossary WordPress plugin before 3.9.21 does not escape some glossary_tooltip shortcode attributes, which could allow users a role as low as Contributor to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2021-24678**	N/A	A-CMI-ENHA-201021/49
cobbler_project					
cobbler					
Improper Control of Generation of Code ('Code Injection')	04-Oct-21	7.5	Cobbler before 3.3.0 allows log poisoning, and resultant Remote Code Execution, via an XMLRPC method that logs to the logfile for template injection. **CVE ID : CVE-2021-40323**	https://github.com/cobbler/cobbler/commit/d8f60bbf14a838c8c8a1dba98086b223e35fe70a	A-COB-COBB-201021/50
Unrestricted Upload of File with Dangerous Type	04-Oct-21	5	Cobbler before 3.3.0 allows arbitrary file write operations via upload_log_data. **CVE ID : CVE-2021-40324**	https://github.com/cobbler/cobbler/commit/d8f60bbf14a838c8c8a1dba98086b223e35fe70a	A-COB-COBB-201021/51
Incorrect Authorization	04-Oct-21	5	Cobbler before 3.3.0 allows authorization bypass for modification of settings. **CVE ID : CVE-2021-40325**	https://github.com/cobbler/cobbler/commit/d8f60bbf14a838c8c8a1dba98086b223e35fe70a	A-COB-COBB-201021/52
codesolz					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
better_find_and_replace					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-21	4.3	The Better Find and Replace WordPress plugin before 1.2.9 does not escape the 's' GET parameter before outputting back in the All Masking Rules page, leading to a Reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24676**	N/A	A-COD-BETT-201021/53
coinmarketstats					
woo-altcoin-payment-gateway					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-21	4.3	The Bitcoin / AltCoin Payment Gateway for WooCommerce WordPress plugin before 1.6.1 does not escape the 's' GET parameter before outputting back in the All Masking Rules page, leading to a Reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24679**	N/A	A-COI-WOO--201021/54
commonwl					
cwlviewer					
Deserialization of Untrusted Data	01-Oct-21	7.5	cwlviewer is a web application to view and share Common Workflow Language workflows. Versions prior to 1.3.1 contain a Deserialization of Untrusted Data vulnerability. Commit number f6066f09edb70033a2ce80200e9fa9e70a5c29de (dated 2021-09-30)	https://github.com/common-workflow-language/cwlviewer/commit/f6066f09edb70033a2ce80200e9fa9e70a5c29de, https://github.com/common-workflow-	A-COM-CWLV-201021/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			contains a patch. There are no available workarounds aside from installing the patch. The SnakeYaml constructor, by default, allows any data to be parsed. To fix the issue the object needs to be created with a `SafeConstructor` object, as seen in the patch. **CVE ID : CVE-2021-41110**	language/cwl viewer/security/advisories /GHSA-7g7j-f5g3-fqp7	
Concrete5					
concrete5					
Server-Side Request Forgery (SSRF)	07-Oct-21	7.5	A Server-Side Request Forgery vulnerability was found in concrete5 < 8.5.5 that allowed a decimal notation encoded IP address to bypass the limitations in place for localhost allowing interaction with local services. Impact can vary depending on services exposed.CVSSv2.0 AV:A/AC:H/PR:H/UI:N/S:U /C:L/I:N/A:N **CVE ID : CVE-2021-22958**	https://documentation.concretecms.org/developers/introduction/version-history/855-release-notes	A-CON-CONC-201021/56
concrete5-legacy_project					
concrete5-legacy					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in concrete/elements/collection_add.php in concrete5-legacy 5.6.4.0 and below allows remote attackers to inject arbitrary web script or HTML via the mode	N/A	A-CON-CONC-201021/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parameter. **CVE ID : CVE-2021-41461**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in concrete/elements/collection_add.php in concrete5-legacy 5.6.4.0 and below allows remote attackers to inject arbitrary web script or HTML via the ctID parameter. **CVE ID : CVE-2021-41462**	N/A	A-CON-CONC-201021/58
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in toos/permissions/dialogs/access/entity/types/group_combination.php in concrete5-legacy 5.6.4.0 and below allows remote attackers to inject arbitrary web script or HTML via the cID parameter. **CVE ID : CVE-2021-41463**	N/A	A-CON-CONC-201021/59
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in concrete/elements/collection_add.php in concrete5-legacy 5.6.4.0 and below allows remote attackers to inject arbitrary web script or HTML via the rel parameter. **CVE ID : CVE-2021-41464**	N/A	A-CON-CONC-201021/60
Improper Neutralization of Input During Web Page Generation	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in concrete/elements/collection_theme.php in concrete5-legacy 5.6.4.0 and below allows remote	N/A	A-CON-CONC-201021/61

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attackers to inject arbitrary web script or HTML via the rel parameter. **CVE ID : CVE-2021-41465**		
Corel					
coreldraw_2020					
Out-of-bounds Read	02-Oct-21	4.3	CdrCore.dll in Corel DrawStandard 2020 22.0.0.474 is affected by an Out-of-bounds Read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious CDR file. **CVE ID : CVE-2021-38107**	N/A	A-COR-CORE-201021/62
Out-of-bounds Read	02-Oct-21	4.3	Corel DrawStandard 2020 22.0.0.474 is affected by an Out-of-bounds Read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious CDR file. **CVE ID : CVE-2021-38109**	N/A	A-COR-CORE-201021/63

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pdf_fusion					
Out-of-bounds Write	01-Oct-21	9.3	Coreip.dll in Corel PDF Fusion 2.6.2.0 is affected by an Out-of-bounds Write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious PDF file. **CVE ID : CVE-2021-38096**	N/A	A-COR-PDF_-201021/64
Out-of-bounds Write	01-Oct-21	9.3	Corel PDF Fusion 2.6.2.0 is affected by an Out-of-bounds Write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious PDF file. **CVE ID : CVE-2021-38097**	N/A	A-COR-PDF_-201021/65
Out-of-bounds Write	01-Oct-21	6.8	Corel PDF Fusion 2.6.2.0 is affected by a Heap Corruption vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve	N/A	A-COR-PDF_-201021/66

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious PDF file. **CVE ID : CVE-2021-38098**		
photopaint_2020					
Out-of-bounds Write	01-Oct-21	9.3	CDRRip.dll in Corel PhotoPaint Standard 2020 22.0.0.474 is affected by an Out-of-bounds Write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious CPT file. This is different from CVE-2021-38101. **CVE ID : CVE-2021-38099**	N/A	A-COR-PHOT-201021/67
Out-of-bounds Write	01-Oct-21	6.8	Corel PhotoPaint Standard 2020 22.0.0.474 is affected by an Out-of-bounds Write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user	N/A	A-COR-PHOT-201021/68

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious CPT file. **CVE ID : CVE-2021-38100**		
Out-of-bounds Write	01-Oct-21	6.8	CDRRip.dll in Corel PhotoPaint Standard 2020 22.0.0.474 is affected by an Out-of-bounds Write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious CPT file. This is different from CVE-2021-38099. **CVE ID : CVE-2021-38101**	N/A	A-COR-PHOT-201021/69
presentations_2020					
Out-of-bounds Read	01-Oct-21	4.3	IPPP82.FLT in Corel Presentations 2020 20.0.0.200 is affected by an Out-of-bounds Read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious PPT file. This is	N/A	A-COR-PRES-201021/70

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			different from CVE-2021-38105. **CVE ID : CVE-2021-38102**		
Out-of-bounds Write	01-Oct-21	9.3	IBJPG2.FLT in Corel Presentations 2020 20.0.0.200 is affected by an Out-of-bounds Write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious PPT file. **CVE ID : CVE-2021-38103**	N/A	A-COR-PRES-201021/71
Out-of-bounds Read	01-Oct-21	4.3	IPPP72.FLT in Corel Presentations 2020 20.0.0.200 is affected by an Out-of-bounds Read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious PPT file. **CVE ID : CVE-2021-38104**	N/A	A-COR-PRES-201021/72
Out-of-bounds Read	01-Oct-21	4.3	IPPP82.FLT in Corel Presentations 2020	N/A	A-COR-PRES-201021/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.0.0.200 is affected by an Out-of-bounds Read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious PPT file. This is different from CVE-2021-38102. **CVE ID : CVE-2021-38105**		
Out-of-bounds Read	01-Oct-21	4.3	UAX200.dll in Corel Presentations 2020 20.0.0.200 is affected by an Out-of-bounds Read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious PPT file. **CVE ID : CVE-2021-38106**	N/A	A-COR-PRES-201021/74
wordperfect_2020					
Out-of-bounds Read	02-Oct-21	4.3	Word97Import200.dll in Corel WordPerfect 2020 20.0.0.200 is affected by an Out-of-bounds Read	N/A	A-COR-WORD-201021/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to access unauthorized system memory in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious DOC file. **CVE ID : CVE-2021-38108**		
Out-of-bounds Write	01-Oct-21	6.8	Word97Import200.dll in Corel WordPerfect 2020 20.0.0.200 is affected by an Out-of-bounds Write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious DOC file. **CVE ID : CVE-2021-38110**	N/A	A-COR-WORD-201021/76
detector_project					
detector					
Improper Neutralization of Input During Web Page Generation ('Cross-site	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in _contactform.inc.php in Detector 0.8.5 and below version allows remote attackers to inject arbitrary web script or HTML via the	N/A	A-DET-DETE-201021/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			cid parameter. **CVE ID : CVE-2021-40921**		
Digi					
realport					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	A-DIG-REAL-201021/78
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	A-DIG-REAL-201021/79
django-unicorn					
unicorn					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-21	3.5	The Unicorn framework through 0.35.3 for Django allows XSS via component.name. **CVE ID : CVE-2021-42053**	https://github.com/adamghill/django-unicorn/pull/288/files, https://github.com/adamghill/django-unicorn/compare/0.35.3...0.36.0	A-DJA-UNIC-201021/80
Docker					
command_line_interface					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	04-Oct-21	5	Docker CLI is the command line interface for the docker container runtime. A bug was found in the Docker CLI where running `docker login my-private-registry.example.com` with a misconfigured configuration file (typically `~/.docker/config.json`) listing a `credsStore` or `credHelpers` that could not be executed would result in any provided credentials being sent to `registry-1.docker.io` rather than the intended private registry. This bug has been fixed in Docker CLI 20.10.9. Users should update to this version as soon as possible. For users unable to update ensure that any configured credsStore or credHelpers entries in the configuration file reference an installed credential helper that is executable and on the PATH. **CVE ID : CVE-2021-41092**	https://github.com/docker/cli/commit/893e52cf4ba4b048d72e99748e0f86b2767c6c6b, https://github.com/docker/cli/security/advisories/GHSA-99pg-grm5-qq3v	A-DOC-COMM-201021/81
duplicatepro					
duplicate_page					
Improper Neutralization of Input During Web Page Generation ('Cross-site	11-Oct-21	3.5	The Duplicate Page WordPress plugin through 4.4.2 does not sanitise or escape the Duplicate Post Suffix settings before outputting it, which could allow high privilege users	N/A	A-DUP-DUPL-201021/82

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
Scripting')			to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24681**		
dwbooster					
appointment_hour_booking					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-21	3.5	The Appointment Hour Booking WordPress plugin before 1.3.16 does not escape some of the Calendar Form settings, allowing high privilege users to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24673**	N/A	A-DWB-APPO-201021/83
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-21	3.5	The Appointment Hour Booking WordPress plugin before 1.3.17 does not properly sanitize values used when creating new calendars. **CVE ID : CVE-2021-24712**	N/A	A-DWB-APPO-201021/84
dynamicpagelist3_project					
dynamicpagelist3					
Uncontrolled Resource Consumption	04-Oct-21	5	The DynamicPageList3 extension is a reporting tool for MediaWiki, listing category members and intersections with various formats and details. In affected versions unsanitised input of regular expression date within the	https://github.com/Universal-Omega/DynamicPageList3/commit/2c04dafb37a14d9ccfe070f53e7f11bbca015	A-DYN-DYNA-201021/85

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parameters of the DPL parser function, allowed for the possibility of ReDoS (Regex Denial of Service). This has been resolved in version 3.3.6. If you are unable to update you may also set `$wgDplSettings['functionalRichness'] = 0;` or disable DynamicPageList3 to mitigate. **CVE ID : CVE-2021-41118**	6e7, https://github.com/Universal-Omega/DynamicPageList3/security/advisories/GHSA-8f24-q75c-jhf4	
ecommerce-codeigniter-bootstrap_project					
ecommerce-codeigniter-bootstrap					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in application/modules/admin/views/ecommerce/products.php in Ecommerce-CodeIgniter-Bootstrap (Codeigniter 3.1.11, Bootstrap 3.3.7) allows remote attackers to inject arbitrary web script or HTML via the search_title parameter. **CVE ID : CVE-2021-40975**	N/A	A-ECO-ECOM-201021/86
Esri					
portal_for_arcgis					
Improper Privilege Management	01-Oct-21	6.5	There is an privilege escalation vulnerability in organization-specific logins in Esri Portal for ArcGIS versions 10.9 and below that may allow a remote, authenticated attacker to impersonate another	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/Portal-for-	A-ESR-PORT-201021/87

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			account. **CVE ID : CVE-2021-29108**	ArcGIS-Security-2021-Update-1-Patch/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	A reflected XSS vulnerability in Esri Portal for ArcGIS version 10.9 and below may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user's browser. **CVE ID : CVE-2021-29109**	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/Portal-for-ArcGIS-Security-2021-Update-1-Patch/	A-ESR-PORT-201021/88
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	3.5	Stored cross-site scripting (XSS) issue in Esri Portal for ArcGIS may allow a remote unauthenticated attacker to pass and store malicious strings in the home application. **CVE ID : CVE-2021-29110**	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/Portal-for-ArcGIS-Security-2021-Update-1-Patch/	A-ESR-PORT-201021/89
expresstech					
quiz_and_survey_master					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-21	3.5	The Quiz And Survey Master WordPress plugin before 7.3.2 does not escape the Quiz Url Slug setting before outputting it in some pages, which could allow high privilege users to perform Cross-Site Scripting attacks even	N/A	A-EXP-QUIZ-201021/90

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24691**		
extendify					
editorskit					
Improper Control of Generation of Code ('Code Injection')	11-Oct-21	6.5	The Gutenberg Block Editor Toolkit â€“ EditorsKit WordPress plugin before 1.31.6 does not sanitise and validate the Conditional Logic of the Custom Visibility settings, allowing users with a role as low contributor to execute Arbitrary PHP code **CVE ID : CVE-2021-24546**	N/A	A-EXT-EDIT-201021/91
F-secure					
atlant					
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVRDL unpacking module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-40832**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40832	A-F-S-ATLA-201021/92
N/A	06-Oct-21	5	A vulnerability affecting the F-Secure Antivirus engine	https://www.f-	A-F-S-ATLA-201021/93

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
			was discovered when the engine tries to unpack a zip archive (LZW decompression method), and this can crash the scanning engine. The vulnerability can be exploited remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine. **CVE ID : CVE-2021-33602**	secure.com/en/business/support-and-downloads/security-advisories	
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVPACK module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33603**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-33603	A-F-S-ATLA-201021/94
cloud_protection					
N/A	06-Oct-21	5	A vulnerability affecting the F-Secure Antivirus engine was discovered when the engine tries to unpack a zip archive (LZW decompression method), and this can crash the scanning engine. The	https://www.f-secure.com/en/business/support-and-downloads/security-	A-F-S-CLOU-201021/95

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can be exploited remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine. **CVE ID : CVE-2021-33602**	advisories	
cloud_protection_for_salesforce					
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVRDL unpacking module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-40832**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40832	A-F-S-CLOU-201021/96
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVPACK module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-	A-F-S-CLOU-201021/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Anti-Virus engine. **CVE ID : CVE-2021-33603**	downloads/security-advisories/cve-2021-33603	
elements_endpoint_detection_and_response					
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVRDL unpacking module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-40832**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40832	A-F-S-ELEM-201021/98
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVPACK module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33603**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cv	A-F-S-ELEM-201021/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				e-2021-33603	
elements_endpoint_protection					
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVRDL unpacking module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-40832**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40832	A-F-S-ELEM-201021/100
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVPACK module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33603**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-33603	A-F-S-ELEM-201021/101
elements_for_microsoft_365					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVRDL unpacking module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-40832**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40832	A-F-S-ELEM-201021/102
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVPACK module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33603**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-33603	A-F-S-ELEM-201021/103
internet_gatekeeper					
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure	https://www.f-secure.com/e	A-F-S-INTE-201021/104

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
			Atlant whereby the AVRDL unpacking module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-40832**	n/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40832	
N/A	06-Oct-21	5	A vulnerability affecting the F-Secure Antivirus engine was discovered when the engine tries to unpack a zip archive (LZW decompression method), and this can crash the scanning engine. The vulnerability can be exploited remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine. **CVE ID : CVE-2021-33602**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories	A-F-S-INTE-201021/105
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVPACK module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.	A-F-S-INTE-201021/106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33603**	f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-33603	
linux_security					
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVRDL unpacking module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-40832**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40832	A-F-S-LINU-201021/107
N/A	06-Oct-21	5	A vulnerability affecting the F-Secure Antivirus engine was discovered when the engine tries to unpack a zip archive (LZW decompression method), and this can crash the scanning engine. The vulnerability can be exploited remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus	https://www.f-secure.com/en/business/support-and-downloads/security-advisories	A-F-S-LINU-201021/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			engine. **CVE ID : CVE-2021-33602**		
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVPACK module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33603**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-33603	A-F-S-LINU-201021/109
faveohelpdesk					
faveo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in dompdf/dompdf/www/demo.php infaveo-helpdesk v1.11.0 and below allow remote attackers to inject arbitrary web script or HTML via the $_SERVER["PHP_SELF"] parameter. **CVE ID : CVE-2021-40925**	N/A	A-FAV-FAVE-201021/110
Flatpak					
Flatpak					
Improper Input Validation	08-Oct-21	4.6	Flatpak is a system for building, distributing, and running sandboxed	https://github.com/flatpak/flatpak/com	A-FLA-FLAT-201021/111

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
			desktop applications on Linux. In versions prior to 1.10.4 and 1.12.0, Flatpak apps with direct access to AF_UNIX sockets such as those used by Wayland, Pipewire or pipewire-pulse can trick portals and other host-OS services into treating the Flatpak app as though it was an ordinary, non-sandboxed host-OS process. They can do this by manipulating the VFS using recent mount-related syscalls that are not blocked by Flatpak's denylist seccomp filter, in order to substitute a crafted `/.flatpak-info` or make that file disappear entirely. Flatpak apps that act as clients for AF_UNIX sockets such as those used by Wayland, Pipewire or pipewire-pulse can escalate the privileges that the corresponding services will believe the Flatpak app has. Note that protocols that operate entirely over the D-Bus session bus (user bus), system bus or accessibility bus are not affected by this. This is due to the use of a proxy process `xdg-dbus-proxy`, whose VFS cannot be manipulated by the Flatpak app, when interacting with these buses. Patches exist for	mit/1330662f33a55e88bfe18e76de28b7922d91a999, https://github.com/flatpak/flatpak/commit/a10f52a7565c549612c92b8e736a6698a53db330, https://github.com/flatpak/flatpak/commit/4c34815784e9ffda5733225c7d95824f96375e36	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions 1.10.4 and 1.12.0, and as of time of publication, a patch for version 1.8.2 is being planned. There are no workarounds aside from upgrading to a patched version. **CVE ID : CVE-2021-41133**		
Foliovision					
fv_flowplayer_video_player					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-21	4.3	The FV Flowplayer Video Player WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the player_id parameter found in the ~/view/stats.php file which allows attackers to inject arbitrary web scripts, in versions 7.5.0.727 - 7.5.2.727. **CVE ID : CVE-2021-39350**	https://plugins.trac.wordpress.org/changeset/2580834/fv-wordpress-flowplayer/trunk/view/stats.php	A-FOL-FV_F-201021/112
forcepoint					
next_generation_firewall					
N/A	04-Oct-21	4.3	Forcepoint NGFW Engine versions 6.5.11 and earlier, 6.8.6 and earlier, and 6.10.0 are vulnerable to TCP reflected amplification vulnerability, if HTTP User Response has been configured. **CVE ID : CVE-2021-41530**	https://help.forcepoint.com/security/CVE/CVE-2021-41530.html	A-FOR-NEXT-201021/113
Fortinet					
fortianalyzer					
Insufficiently Protected	06-Oct-21	2.1	An information disclosure vulnerability [CWE-200] in	https://fortiguard.com/adv	A-FOR-FORT-201021/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			FortiAnalyzerVM and FortiManagerVM versions 7.0.0 and 6.4.6 and below may allow an authenticated attacker to read the FortiCloud credentials which were used to activate the trial license in cleartext. **CVE ID : CVE-2021-36170**	isory/FG-IR-21-112	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-21	3.5	An improper neutralization of input vulnerability [CWE-79] in FortiAnalyzer versions 6.4.3 and below, 6.2.7 and below and 6.0.10 and below may allow a remote authenticated attacker to perform a stored cross site scripting attack (XSS) via the column settings of Logview in FortiAnalyzer, should the attacker be able to obtain that POST request, via other, hypothetical attacks. **CVE ID : CVE-2021-24021**	https://fortiguard.com/advisory/FG-IR-20-098	A-FOR-FORT-201021/115
forticlient_endpoint_management_server					
Insufficient Session Expiration	06-Oct-21	7.5	An insufficient session expiration vulnerability [CWE- 613] in FortiClientEMS versions 6.4.2 and below, 6.2.8 and below may allow an attacker to reuse the unexpired admin user session IDs to gain admin privileges, should the attacker be able to obtain that session ID (via other,	https://fortiguard.com/advisory/FG-IR-20-072	A-FOR-FORT-201021/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hypothetical attacks) **CVE ID : CVE-2021-24019**		
fortimanager					
Insufficiently Protected Credentials	06-Oct-21	2.1	An information disclosure vulnerability [CWE-200] in FortiAnalyzerVM and FortiManagerVM versions 7.0.0 and 6.4.6 and below may allow an authenticated attacker to read the FortiCloud credentials which were used to activate the trial license in cleartext. **CVE ID : CVE-2021-36170**	https://fortiguard.com/advisory/FG-IR-21-112	A-FOR-FORT-201021/117
fortisdnconnector					
Insufficiently Protected Credentials	06-Oct-21	4	A insufficiently protected credentials in Fortinet FortiSDNConnector version 1.1.7 and below allows attacker to disclose third-party devices credential information via configuration page lookup. **CVE ID : CVE-2021-36178**	https://fortiguard.com/advisory/FG-IR-20-183	A-FOR-FORT-201021/118
fortiweb					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-21	3.5	An improper neutralization of input vulnerability [CWE-79] in FortiWebManager versions 6.2.3 and below, 6.0.2 and below may allow a remote authenticated attacker to inject malicious script/tags via the name/description/comments parameter of various sections of the device.	https://fortiguard.com/advisory/FG-IR-20-027	A-FOR-FORT-201021/119

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-2021-36175		
frontend_uploader_project					
frontend_uploader					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-21	4.3	The Frontend Uploader WordPress plugin through 1.3.2 does not prevent HTML files from being uploaded via its form, allowing unauthenticated user to upload a malicious HTML file containing JavaScript for example, which will be triggered when someone access the file directly **CVE ID : CVE-2021-24563**	N/A	A-FRO-FRON-201021/120
galera					
galera_webtemplate					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Oct-21	7.5	Galera WebTemplate 1.0 is affected by a directory traversal vulnerability that could reveal information from /etc/passwd and /etc/shadow. **CVE ID : CVE-2021-40960**	N/A	A-GAL-GALE-201021/121
gclib_project					
gclib					
Out-of-bounds Read	04-Oct-21	6.8	An out-of-bounds access in GffLine::GffLine in gff.cpp in GCLib 0.12.7 allows an attacker to cause a segmentation fault or possibly have unspecified other impact via a crafted GFF file. **CVE ID : CVE-2021-42006**	https://github.com/gpertea/gclib/issues/11	A-GCL-GCLI-201021/122

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
getcomposer					
composer					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Oct-21	7.5	Composer is an open source dependency manager for the PHP language. In affected versions windows users running Composer to install untrusted dependencies are subject to command injection and should upgrade their composer version. Other OSs and WSL are not affected. The issue has been resolved in composer versions 1.10.23 and 2.1.9. There are no workarounds for this issue. **CVE ID : CVE-2021-41116**	https://github.com/composer/composer/commit/ca5e2f8d505fd3bfac6f7c85b82f2740becbc0aa, https://github.com/composer/composer/security/advisories/GHSA-frqg-7g38-6gcf	A-GET-COMP-201021/123
Getid3					
getid3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in demos/demo.mysqli.php in getID3 1.X and v2.0.0-beta allows remote attackers to inject arbitrary web script or HTML via the showtagfiles parameter. **CVE ID : CVE-2021-40926**	N/A	A-GET-GETI-201021/124
gfos					
workforce_management					
Improper Authentication	04-Oct-21	6.8	In GFOS Workforce Management 4.8.272.1, the login page of application is prone to authentication bypass, allowing anyone	N/A	A-GFO-WORK-201021/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(who knows a user's credentials except the password) to get access to an account. This occurs because of JSESSIONID mismanagement. **CVE ID : CVE-2021-38618**		
gilacms					
gila_cms					
Exposure of Sensitive Information to an Unauthorized Actor	04-Oct-21	5	Gila CMS 2.2.0 is vulnerable to Insecure Direct Object Reference (IDOR). Thumbnails uploaded by one site owner are visible by another site owner just by knowing the other site name and fuzzing for picture names. This leads to sensitive information disclosure. **CVE ID : CVE-2021-37777**	N/A	A-GIL-GILA-201021/126
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-21	3.5	A Stored XSS via Malicious File Upload exists in Gila CMS version 2.2.0. An attacker can use this to steal cookies, passwords or to run arbitrary code on a victim's browser. **CVE ID : CVE-2021-39486**	N/A	A-GIL-GILA-201021/127
Gitlab					
gitlab					
Exposure of Resource to Wrong Sphere	05-Oct-21	5.5	A business logic error in the project deletion process in GitLab 13.6 and later allows persistent access via project access tokens.	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39866.json	A-GIT-GITL-201021/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39866		
Server-Side Request Forgery (SSRF)	05-Oct-21	5.5	In all versions of GitLab CE/EE since version 8.15, a DNS rebinding vulnerability in Gitea Importer may be exploited by an attacker to trigger Server Side Request Forgery (SSRF) attacks. **CVE ID : CVE-2021-39867**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39867.json	A-GIT-GITL-201021/129
Incorrect Permission Assignment for Critical Resource	04-Oct-21	4	In all versions of GitLab CE/EE since version 8.12, an authenticated low-privileged malicious user may create a project with unlimited repository size by modifying values in a project export. **CVE ID : CVE-2021-39868**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39868.json	A-GIT-GITL-201021/130
Exposure of Sensitive Information to an Unauthorized Actor	05-Oct-21	4.3	In all versions of GitLab CE/EE since version 8.9, project exports may expose trigger tokens configured on that project. **CVE ID : CVE-2021-39869**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39869.json	A-GIT-GITL-201021/131
N/A	05-Oct-21	4	In all versions of GitLab CE/EE since version 11.11, an instance that has the setting to disable Repo by URL import enabled is bypassed by an attacker making a crafted API call. **CVE ID : CVE-2021-39870**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39870.json	A-GIT-GITL-201021/132
N/A	04-Oct-21	4	In all versions of GitLab CE/EE since version 13.0, an instance that has the setting to disable Bitbucket	https://gitlab.com/gitlab-org/cves/-/blob/master	A-GIT-GITL-201021/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server import enabled is bypassed by an attacker making a crafted API call. **CVE ID : CVE-2021-39871**	/2021/CVE-2021-39871.json	
Improper Authentication	05-Oct-21	4	In all versions of GitLab CE/EE since version 14.1, an improper access control vulnerability allows users with expired password to still access GitLab through git and API through access tokens acquired before password expiration. **CVE ID : CVE-2021-39872**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39872.json	A-GIT-GITL-201021/134
N/A	04-Oct-21	4.3	In all versions of GitLab CE/EE, there exists a content spoofing vulnerability which may be leveraged by attackers to trick users into visiting a malicious website by spoofing the content in an error response. **CVE ID : CVE-2021-39873**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39873.json	A-GIT-GITL-201021/135
N/A	04-Oct-21	4	In all versions of GitLab CE/EE since version 11.0, the requirement to enforce 2FA is not honored when using git commands. **CVE ID : CVE-2021-39874**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39874.json	A-GIT-GITL-201021/136
Exposure of Sensitive Information to an Unauthorized Actor	05-Oct-21	5	In all versions of GitLab CE/EE since version 13.6, it is possible to see pending invitations of any public group or public project by visiting an API endpoint. **CVE ID : CVE-2021-39875**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39875.json	A-GIT-GITL-201021/137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	04-Oct-21	4.3	A vulnerability was discovered in GitLab starting with version 12.2 that allows an attacker to cause uncontrolled resource consumption with a specially crafted file. **CVE ID : CVE-2021-39877**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39877.json	A-GIT-GITL-201021/138
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Oct-21	3.5	A stored Reflected Cross-Site Scripting vulnerability in the Jira integration in GitLab version 13.0 up to 14.3.1 allowed an attacker to execute arbitrary javascript code. **CVE ID : CVE-2021-39878**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39878.json	A-GIT-GITL-201021/139
Missing Authentication for Critical Function	04-Oct-21	4	Missing authentication in all versions of GitLab CE/EE since version 7.11.0 allows an attacker with access to a victim's session to disable two-factor authentication **CVE ID : CVE-2021-39879**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39879.json	A-GIT-GITL-201021/140
N/A	05-Oct-21	4	A Denial Of Service vulnerability in the apollo_upload_server Ruby gem in GitLab CE/EE version 11.11 and above allows an attacker to deny access to all users via specially crafted requests to the apollo_upload_server middleware. **CVE ID : CVE-2021-39880**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39880.json	A-GIT-GITL-201021/141
N/A	05-Oct-21	3.5	In all versions of GitLab CE/EE since version 7.7, the application may let a malicious user create an	https://gitlab.com/gitlab-org/cves/-/blob/master	A-GIT-GITL-201021/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OAuth client application with arbitrary scope names which may allow the malicious user to trick unsuspecting users to authorize the malicious client application using the spoofed scope name and description. **CVE ID : CVE-2021-39881**	/2021/CVE-2021-39881.json	
Cleartext Transmission of Sensitive Information	05-Oct-21	5	In all versions of GitLab CE/EE, provided a user ID, anonymous users can use a few endpoints to retrieve information about any GitLab user. **CVE ID : CVE-2021-39882**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39882.json	A-GIT-GITL-201021/143
Incorrect Authorization	04-Oct-21	4	Improper authorization checks in GitLab EE > 13.11 allows subgroup members to see epics from all parent subgroups. **CVE ID : CVE-2021-39883**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39883.json	A-GIT-GITL-201021/144
Exposure of Resource to Wrong Sphere	05-Oct-21	4	In all versions of GitLab EE since version 8.13, an endpoint discloses names of private groups that have access to a project to low privileged users that are part of that project. **CVE ID : CVE-2021-39884**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39884.json	A-GIT-GITL-201021/145
Improper Neutralization of Input During Web Page Generation ('Cross-site	04-Oct-21	3.5	A Stored XSS in merge request creation page in Gitlab EE version 13.5 and above allows an attacker to execute arbitrary JavaScript code on the victim's behalf via	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39885.json	A-GIT-GITL-201021/146

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
Scripting')			malicious approval rule names **CVE ID : CVE-2021-39885**		
Incorrect Default Permissions	05-Oct-21	4	Permissions rules were not applied while issues were moved between projects of the same group in GitLab versions starting with 10.6 and up to 14.1.7 allowing users to read confidential Epic references. **CVE ID : CVE-2021-39886**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39886.json	A-GIT-GITL-201021/147
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Oct-21	3.5	A stored Cross-Site Scripting vulnerability in the GitLab Flavored Markdown in GitLab CE/EE version 8.4 and above allowed an attacker to execute arbitrary JavaScript code on the victim's behalf. **CVE ID : CVE-2021-39887**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39887.json	A-GIT-GITL-201021/148
Exposure of Sensitive Information to an Unauthorized Actor	05-Oct-21	4	In all versions of GitLab EE since version 13.10, a specific API endpoint may reveal details about a private group and other sensitive info inside issue and merge request templates. **CVE ID : CVE-2021-39888**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39888.json	A-GIT-GITL-201021/149
Incorrect Permission Assignment for Critical Resource	05-Oct-21	4	In all versions of GitLab EE since version 14.1, due to an insecure direct object reference vulnerability, an endpoint may reveal the protected branch name to a malicious user who makes a crafted API call with the	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39889.json	A-GIT-GITL-201021/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID of the protected branch. **CVE ID : CVE-2021-39889**		
Incorrect Authorization	05-Oct-21	4	In all versions of GitLab CE/EE since version 8.0, access tokens created as part of admin's impersonation of a user are not cleared at the end of impersonation which may lead to unnecessary sensitive info disclosure. **CVE ID : CVE-2021-39891**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39891.json	A-GIT-GITL-201021/151
Missing Authorization	05-Oct-21	5	A potential DOS vulnerability was discovered in GitLab starting with version 9.1 that allowed parsing files without authorisation. **CVE ID : CVE-2021-39893**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39893.json	A-GIT-GITL-201021/152
Server-Side Request Forgery (SSRF)	05-Oct-21	5.5	In all versions of GitLab CE/EE since version 8.0, a DNS rebinding vulnerability exists in Fogbugz importer which may be used by attackers to exploit Server Side Request Forgery attacks. **CVE ID : CVE-2021-39894**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39894.json	A-GIT-GITL-201021/153
N/A	04-Oct-21	5.5	In all versions of GitLab CE/EE since version 8.0, when an admin uses the impersonate feature twice and stops impersonating, the admin may be logged in as the second user they impersonated, which may lead to repudiation issues. **CVE ID : CVE-2021-39896**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39896.json	A-GIT-GITL-201021/154

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
Weak Password Recovery Mechanism for Forgotten Password	04-Oct-21	1.9	In all versions of GitLab CE/EE, an attacker with physical access to a user's machine may brute force the user's password via the change password function. There is a rate limit in place, but the attack may still be conducted by stealing the session id from the physical compromise of the account and splitting the attack over several IP addresses and passing in the compromised session value from these various locations. **CVE ID : CVE-2021-39899**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39899.json	A-GIT-GITL-201021/155
Exposure of Resource to Wrong Sphere	04-Oct-21	4	Information disclosure from SendEntry in GitLab starting with 10.8 allowed exposure of full URL of artifacts stored in object-storage with a temporary availability via Rails logs. **CVE ID : CVE-2021-39900**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39900.json	A-GIT-GITL-201021/156
N/A	05-Oct-21	5	An issue has been discovered in GitLab affecting all versions starting from 14.0 before 14.0.9, all versions starting from 14.1 before 14.1.4, all versions starting from 14.2 before 14.2.2. The route for /user.keys is not restricted on instances with public visibility disabled. This allows user enumeration on such instances.	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22257.json	A-GIT-GITL-201021/157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22257		
N/A	05-Oct-21	4	The project import/export feature in GitLab 8.9 and greater could be used to obtain otherwise private email addresses **CVE ID : CVE-2021-22258**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22258.json	A-GIT-GITL-201021/158
N/A	04-Oct-21	4	A potential DOS vulnerability was discovered in GitLab EE starting with version 12.6 due to lack of pagination in dependencies API. **CVE ID : CVE-2021-22259**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22259.json	A-GIT-GITL-201021/159
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Oct-21	3.5	A stored Cross-Site Scripting vulnerability in the Jira integration in GitLab version 13.7 and above allows an attacker to execute arbitrary JavaScript code on the victim's behalf via malicious Jira API responses **CVE ID : CVE-2021-22261**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22261.json	A-GIT-GITL-201021/160
Incorrect Authorization	05-Oct-21	5	Missing access control in GitLab version 13.10 and above with Jira Cloud integration enabled allows Jira users without administrative privileges to add and remove Jira Connect Namespaces via the GitLab.com for Jira Cloud application configuration page **CVE ID : CVE-2021-22262**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22262.json	A-GIT-GITL-201021/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Oct-21	4.3	An issue has been discovered in GitLab affecting all versions starting from 13.8 before 14.0.9, all versions starting from 14.1 before 14.1.4, all versions starting from 14.2 before 14.2.2. Under specialized conditions, an invited group member may continue to have access to a project even after the invited group, which the member was part of, is deleted. **CVE ID : CVE-2021-22264**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22264.json	A-GIT-GITL-201021/162
glimmrtv					
flextv					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in index.php in FlexTV beta development version allows remote attackers to inject arbitrary web script or HTML via the PHP_SELF parameter. **CVE ID : CVE-2021-40928**	N/A	A-GLI-FLEX-201021/163
Google					
chrome					
Use After Free	08-Oct-21	6.8	Use after free in Offline use in Google Chrome on Android prior to 94.0.4606.54 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.	A-GOO-CHRO-201021/164

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-2021-37956	com/1243117	
Use After Free	08-Oct-21	6.8	Use after free in WebGPU in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37957**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1242269	A-GOO-CHRO-201021/165
N/A	08-Oct-21	5.8	Inappropriate implementation in Navigation in Google Chrome on Windows prior to 94.0.4606.54 allowed a remote attacker to inject scripts or HTML into a privileged page via a crafted HTML page. **CVE ID : CVE-2021-37958**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1223290	A-GOO-CHRO-201021/166
Use After Free	08-Oct-21	6.8	Use after free in Task Manager in Google Chrome prior to 94.0.4606.54 allowed an attacker who convinced a user to enage in a series of user gestures to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37959**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1229625	A-GOO-CHRO-201021/167
Use After Free	08-Oct-21	6.8	Use after free in Tab Strip in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37961**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html,	A-GOO-CHRO-201021/168

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
				https://crbug.com/1228557	
Use After Free	08-Oct-21	6.8	Use after free in Performance Manager in Google Chrome prior to 94.0.4606.54 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37962**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1231933	A-GOO-CHRO-201021/169
N/A	08-Oct-21	4.3	Side-channel information leakage in DevTools in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to bypass site isolation via a crafted HTML page. **CVE ID : CVE-2021-37963**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1199865	A-GOO-CHRO-201021/170
N/A	08-Oct-21	4.3	Inappropriate implementation in ChromeOS Networking in Google Chrome on ChromeOS prior to 94.0.4606.54 allowed an attacker with a rogue wireless access point to to potentially carryout a wifi impersonation attack via a crafted ONC file. **CVE ID : CVE-2021-37964**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1203612	A-GOO-CHRO-201021/171
Exposure of Resource to Wrong Sphere	08-Oct-21	4.3	Inappropriate implementation in Background Fetch API in Google Chrome prior to 94.0.4606.54 allowed a	https://chromereleases.googleblog.com/2021/09/stable-channel-	A-GOO-CHRO-201021/172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-37965**	update-for-desktop_21.html, https://crbug.com/1239709	
Origin Validation Error	08-Oct-21	4.3	Inappropriate implementation in Compositing in Google Chrome on Android prior to 94.0.4606.54 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-37966**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1238944	A-GOO-CHRO-201021/173
Exposure of Resource to Wrong Sphere	08-Oct-21	4.3	Inappropriate implementation in Background Fetch API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-37967**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1243622	A-GOO-CHRO-201021/174
Exposure of Resource to Wrong Sphere	08-Oct-21	4.3	Inappropriate implementation in Background Fetch API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-37968**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1245053	A-GOO-CHRO-201021/175
Improper Privilege Management	08-Oct-21	6.8	Inappropriate implementation in Google Updater in Google Chrome	https://chromereleases.googleblog.com/	A-GOO-CHRO-201021/176

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
			on Windows prior to 94.0.4606.54 allowed a remote attacker to perform local privilege escalation via a crafted file. **CVE ID : CVE-2021-37969**	2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1245879	
Use After Free	08-Oct-21	6.8	Use after free in File System API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37970**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1248030	A-GOO-CHRO-201021/177
Origin Validation Error	08-Oct-21	4.3	Incorrect security UI in Web Browser UI in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-37971**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1219354	A-GOO-CHRO-201021/178
Out-of-bounds Read	08-Oct-21	6.8	Out of bounds read in libjpeg-turbo in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37972**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1234259	A-GOO-CHRO-201021/179
Use After Free	08-Oct-21	6.8	Use after free in Portals in Google Chrome prior to 94.0.4606.61 allowed a	https://chromereleases.googleblog.com/	A-GOO-CHRO-201021/180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2021-37973**	2021/09/stable-channel-update-for-desktop_24.html, https://crbug.com/1251727	
Use After Free	08-Oct-21	6.8	Use after free in Safebrowsing in Google Chrome prior to 94.0.4606.71 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37974**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_30.html, https://crbug.com/1245578	A-GOO-CHRO-201021/181
Use After Free	08-Oct-21	6.8	Use after free in V8 in Google Chrome prior to 94.0.4606.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37975**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_30.html, https://crbug.com/1252918	A-GOO-CHRO-201021/182
N/A	08-Oct-21	4.3	Inappropriate implementation in Memory in Google Chrome prior to 94.0.4606.71 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. **CVE ID : CVE-2021-37976**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_30.html, https://crbug.com/1251787	A-GOO-CHRO-201021/183
Use After Free	08-Oct-21	6.8	Use after free in Selection API in Google Chrome prior	https://crbug.com/1237533	A-GOO-CHRO-201021/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 93.0.4577.82 allowed a remote attacker who convinced the user the visit a malicious website to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30625**	, https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Oct-21	6.8	Out of bounds memory access in ANGLE in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30626**	https://crbug.com/1241036 , https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	A-GOO-CHRO-201021/185
Access of Resource Using Incompatible Type ('Type Confusion')	08-Oct-21	6.8	Type confusion in Blink layout in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30627**	https://crbug.com/1245786 , https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	A-GOO-CHRO-201021/186
Out-of-bounds Write	08-Oct-21	6.8	Stack buffer overflow in ANGLE in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page. **CVE ID : CVE-2021-30628**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html, https://crbug.com/1241123	A-GOO-CHRO-201021/187
Use After Free	08-Oct-21	6.8	Use after free in Permissions in Google	https://crbug.com/1243646	A-GOO-CHRO-201021/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Chrome prior to 93.0.4577.82 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30629**	, https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	
Exposure of Resource to Wrong Sphere	08-Oct-21	4.3	Inappropriate implementation in Blink in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-30630**	https://crbug.com/1244568 , https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	A-GOO-CHRO-201021/189
Out-of-bounds Write	08-Oct-21	6.8	Out of bounds write in V8 in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30632**	https://crbug.com/1247763 , https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	A-GOO-CHRO-201021/190
Use After Free	08-Oct-21	6.8	Use after free in Indexed DB API in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2021-30633**	https://crbug.com/1247766 , https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	A-GOO-CHRO-201021/191
slo_generator					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	04-Oct-21	6.8	SLO generator allows for loading of YAML files that if crafted in a specific format can allow for code execution within the context of the SLO Generator. We recommend upgrading SLO Generator past https://github.com/google/slo-generator/pull/173 **CVE ID : CVE-2021-22557**	https://github.com/google/slo-generator/pull/173	A-GOO-SLO_-201021/192
gpac					
mp4box					
Out-of-bounds Write	01-Oct-21	5	There is a stack buffer overflow in MP4Box v1.0.1 at src/filters/dmx_nhml.c:1004 in the nhmldmx_send_sample() function szXmlTo parameter which leads to a denial of service vulnerability. **CVE ID : CVE-2021-41456**	N/A	A-GPA-MP4B-201021/193
Out-of-bounds Write	01-Oct-21	5	There is a stack buffer overflow in MP4Box 1.1.0 at src/filters/dmx_nhml.c in nhmldmx_init_parsing which leads to a denial of service vulnerability. **CVE ID : CVE-2021-41457**	N/A	A-GPA-MP4B-201021/194
Out-of-bounds Write	01-Oct-21	5	There is a stack buffer overflow in MP4Box v1.0.1 at src/filters/dmx_nhml.c:1008 in the nhmldmx_send_sample()	N/A	A-GPA-MP4B-201021/195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function szXmlFrom parameter which leads to a denial of service vulnerability. **CVE ID : CVE-2021-41459**		
grafana					
grafana					
Improper Authentication	05-Oct-21	6.8	Grafana is an open source data visualization platform. In affected versions unauthenticated and authenticated users are able to view the snapshot with the lowest database key by accessing the literal paths: /dashboard/snapshot/:key , or /api/snapshots/:key. If the snapshot "public_mode" configuration setting is set to true (vs default of false), unauthenticated users are able to delete the snapshot with the lowest database key by accessing the literal path: /api/snapshots-delete/:deleteKey. Regardless of the snapshot "public_mode" setting, authenticated users are able to delete the snapshot with the lowest database key by accessing the literal paths: /api/snapshots/:key, or /api/snapshots-delete/:deleteKey. The combination of deletion and viewing enables a	https://github.com/grafana/grafana/commit/2d456a6375855364d098ede379438bf7f0667269, https://grafana.com/docs/grafana/latest/release-notes/release-notes-8-1-6/, https://github.com/grafana/grafana/security/advisories/GHSA-69j6-29vr-p3j9	A-GRA-GRAF-201021/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			complete walk through all snapshot data while resulting in complete snapshot data loss. This issue has been resolved in versions 8.1.6 and 7.5.11. If for some reason you cannot upgrade you can use a reverse proxy or similar to block access to the literal paths: /api/snapshots/:key, /api/snapshots-delete/:deleteKey, /dashboard/snapshot/:key, and /api/snapshots/:key. They have no normal function and can be disabled without side effects. **CVE ID : CVE-2021-39226**		
gvectors					
wpdiscuz					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-21	3.5	The Comments â€“ wpDiscuz WordPress plugin through 7.3.0 does not properly sanitise or escape the Follow and Unfollow messages before outputting them in the page, which could allow high privilege users to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24737**	N/A	A-GVE-WPDI-201021/197
hashicorp					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nomad					
N/A	07-Oct-21	4	HashiCorp Nomad and Nomad Enterprise 1.1.1 through 1.1.5 allowed authenticated users with job submission capabilities to cause denial of service by submitting incomplete job specifications with a Consul mesh gateway and host networking mode. Fixed in 1.1.6. **CVE ID : CVE-2021-41865**	https://discuss.hashicorp.com/t/hcsec-2021-26-nomad-denial-of-service-via-submission-of-incomplete-job-specification-using-consul-mesh-gateway-host-network/30311	A-HAS-NOMA-201021/198
hkurl					
i-panel_administration_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-21	4.3	A reflected cross-site scripting (XSS) vulnerability exists in the i-Panel Administration System Version 2.0 that enables a remote attacker to execute arbitrary JavaScript code in the browser-based web console and it is possible to insert a vulnerable malicious button. **CVE ID : CVE-2021-41878**	N/A	A-HKU-I-PA-201021/199
hotel_management_system_project					
hotel_management_system					
Improper Neutralization of Special	04-Oct-21	5	A blind SQL injection vulnerability exists in the Raymart DG / Ahmed Helal	N/A	A-HOT-HOTE-201021/200

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
Elements used in an SQL Command ('SQL Injection')			Hotel-mgmt-system. A malicious attacker can retrieve sensitive database information and interact with the database using the vulnerable cid parameter in process_update_profile.php . **CVE ID : CVE-2021-41651**		
hygeia_project					
hygeia					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Oct-21	6.5	Hygeia is an application for collecting and processing personal and case data in connection with communicable diseases. In affected versions all CSV Exports (Statistics & BAG MED) contain a CSV Injection Vulnerability. Users of the system are able to submit formula as exported fields which then get executed upon ingestion of the exported file. There is no validation or sanitization of these formula fields and so malicious may construct malicious code. This vulnerability has been resolved in version 1.30.4. There are no workarounds and all users are advised to upgrade their package. **CVE ID : CVE-2021-41128**	https://github.com/jshmrtn/hygeia/commit/d917f27432fe84e1c9751222ae55bae36a4dce60, https://github.com/jshmrtn/hygeia/security/advisories/GHSA-8pwv-jhj2-2369	A-HYG-HYGE-201021/201
IBM					
app_connect_enterprise_certified_container					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Oct-21	1.9	IBM App Connect Enterprise Certified Container 1.0, 1.1, 1.2, 1.3, 1.4 and 1.5 could disclose sensitive information to a local user when it is configured to use an IBM Cloud API key to connect to cloud-based connectors. IBM X-Force ID: 207630. **CVE ID : CVE-2021-29906**	https://www.ibm.com/support/pages/node/6497177, https://exchange.xforce.ibmcloud.com/vulnerabilities/207630	A-IBM-APP_-201021/202
sterling_b2b_integrator					
Inadequate Encryption Strength	06-Oct-21	5	IBM Sterling B2B Integrator Standard Edition 5.2.0. 0 through 6.1.1.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 210171. **CVE ID : CVE-2021-38925**	https://www.ibm.com/support/pages/node/6495905, https://exchange.xforce.ibmcloud.com/vulnerabilities/210171	A-IBM-STER-201021/203
Improper Authentication	07-Oct-21	4	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 could allow a remote authenticated user to cause a denial of another user's service due to insufficient permission checking. IBM X-Force ID: 195518. **CVE ID : CVE-2021-20372**	https://exchange.xforce.ibmcloud.com/vulnerabilities/195518, https://www.ibm.com/support/pages/node/6496805	A-IBM-STER-201021/204
Improper Authentication	07-Oct-21	4	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 could allow an authenticated user to intercept and replace a message sent by another user due to improper access controls. IBM X-	https://www.ibm.com/support/pages/node/6496803, https://exchange.xforce.ibmcloud.com/vulnerabilities/	A-IBM-STER-201021/205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Force ID: 195567. **CVE ID : CVE-2021-20375**	195567	
Exposure of Sensitive Information to an Unauthorized Actor	07-Oct-21	4	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 could allow an authenticated attacker to enumerate usernames due to there being an observable discrepancy in returned messages. IBM X-Force ID: 195568. **CVE ID : CVE-2021-20376**	https://www.ibm.com/support/pages/node/6496789, https://exchange.xforce.ibmcloud.com/vulnerabilities/195568	A-IBM-STER-201021/206
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-21	4.3	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199230. **CVE ID : CVE-2021-20561**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199230, https://www.ibm.com/support/pages/node/6496759	A-IBM-STER-201021/207
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-21	3.5	IBM Sterling B2B Integrator 5.2.0.0 through 6.1.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199246. **CVE ID : CVE-2021-20571**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199246, https://www.ibm.com/support/pages/node/6496753	A-IBM-STER-201021/208

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
Unrestricted Upload of File with Dangerous Type	07-Oct-21	5	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 could allow a remote attacker to upload arbitrary files, caused by improper access controls. IBM X-Force ID: 199397. **CVE ID : CVE-2021-20584**	https://www.ibm.com/support/pages/node/6496751, https://exchange.xforce.ibmcloud.com/vulnerabilities/199397	A-IBM-STER-201021/209
Exposure of Sensitive Information to an Unauthorized Actor	07-Oct-21	4	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.1.1.0 could allow an authneticated attacker to obtain sensitive information from configuration files that could aid in further attacks against the system. IBM X-Force ID: 200656. **CVE ID : CVE-2021-29700**	https://www.ibm.com/support/pages/node/6496749, https://exchange.xforce.ibmcloud.com/vulnerabilities/200656	A-IBM-STER-201021/210
Improper Authentication	06-Oct-21	4	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.1.1.0 could allow an authenticated user to perform actions that they should not be able to access due to improper access controls. IBM X-Force ID: 202169. **CVE ID : CVE-2021-29758**	https://www.ibm.com/support/pages/node/6495969, https://exchange.xforce.ibmcloud.com/vulnerabilities/202169	A-IBM-STER-201021/211
Incorrect Authorization	06-Oct-21	4	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.1.1.0 could allow an authenticated user to download unauthorized files through the dashboard	https://www.ibm.com/support/pages/node/6495969, https://exchange.xforce.ibmcloud.com/v	A-IBM-STER-201021/212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user interface. IBM X-Force ID: 202213. **CVE ID : CVE-2021-29760**	ulnerabilities/202213	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.1.1.0 could allow an authenticated user to obtain sensitive information from the dashboard that they should not have access to. IBM X-Force ID: 202265. **CVE ID : CVE-2021-29761**	https://www.ibm.com/support/pages/node/6495969, https://exchange.xforce.ibmcloud.com/vulnerabilities/202265	A-IBM-STER-201021/213
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-21	3.5	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.1.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 202268. **CVE ID : CVE-2021-29764**	https://exchange.xforce.ibmcloud.com/vulnerabilities/202268, https://www.ibm.com/support/pages/node/6495967	A-IBM-STER-201021/214
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-21	7.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.1.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-	https://www.ibm.com/support/pages/node/6495925, https://exchange.xforce.ibmcloud.com/vulnerabilities/203734	A-IBM-STER-201021/215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			end database. IBM X-Force ID: 203734. **CVE ID : CVE-2021-29798**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-21	3.5	IBM Sterling B2B Integrator Standard Edition 5.2.0.0. through 6.1.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204912. **CVE ID : CVE-2021-29836**	https://www.ibm.com/support/pages/node/6495921, https://exchange.xforce.ibmcloud.com/vulnerabilities/204912	A-IBM-STER-201021/216
Cross-Site Request Forgery (CSRF)	06-Oct-21	6.8	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.1.1.0 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: 204913. **CVE ID : CVE-2021-29837**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204913, https://www.ibm.com/support/pages/node/6495907	A-IBM-STER-201021/217
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-21	3.5	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.1.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to	https://exchange.xforce.ibmcloud.com/vulnerabilities/205684, https://www.ibm.com/support/pages/node/6495965	A-IBM-STER-201021/218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials disclosure within a trusted session. IBM X-Force ID: 205684. **CVE ID : CVE-2021-29855**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-21	7.5	IBM Sterling B2B Integrator Standard Edition 5.2.6.0 through 6.1.1.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 207506. **CVE ID : CVE-2021-29903**	https://www.ibm.com/support/pages/node/6495919, https://exchange.xforce.ibmcloud.com/vulnerabilities/207506	A-IBM-STER-201021/219
sterling_file_gateway					
Insufficient Session Expiration	07-Oct-21	4	IBM Sterling File Gateway User Interface 2.2.0.0 through 6.1.1.0 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 196944. **CVE ID : CVE-2021-20473**	https://www.ibm.com/support/pages/node/6496785, https://exchange.xforce.ibmcloud.com/vulnerabilities/196944	A-IBM-STER-201021/220
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-21	4.3	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	https://www.ibm.com/support/pages/node/6496781, https://exchange.xforce.ibmcloud.com/vulnerabilities/197503	A-IBM-STER-201021/221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 197503. **CVE ID : CVE-2021-20481**		
Cross-Site Request Forgery (CSRF)	07-Oct-21	6.8	IBM Sterling File Gateway 2.2.0.0 through 6.1.1.0 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: 197790. **CVE ID : CVE-2021-20489**	https://exchange.xforce.ibmcloud.com/vulnerabilities/197790, https://www.ibm.com/support/pages/node/6496777	A-IBM-STER-201021/222
Generation of Error Message Containing Sensitive Information	07-Oct-21	4	IBM Sterling File Gateway 6.0.0.0 through 6.1.1.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 199170. **CVE ID : CVE-2021-20552**	https://www.ibm.com/support/pages/node/6496771, https://exchange.xforce.ibmcloud.com/vulnerabilities/199170	A-IBM-STER-201021/223
icehrm					
icehrm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-21	3.5	A Stored Cross Site Scripting vulnerability via Malicious File Upload exists in multiple pages of IceHrm 30.0.0.OS that allows for arbitrary execution of JavaScript commands. **CVE ID : CVE-2021-38822**	N/A	A-ICE-ICEH-201021/224
Insufficient Session Expiration	04-Oct-21	7.5	The IceHrm 30.0.0 OS website was found vulnerable to Session	N/A	A-ICE-ICEH-201021/225

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
			Management Issue. A signout from an admin account does not invalidate an admin session that is opened in a different browser. **CVE ID : CVE-2021-38823**		
Intelliants					
subrion_cms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Oct-21	6.5	A SQL injection vulnerability exists in Subrion CMS v4.2.1 in the visual-mode. **CVE ID : CVE-2021-41947**	N/A	A-INT-SUBR-201021/226
Jenkins					
git					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-21	4.3	Jenkins Git Plugin 4.8.2 and earlier does not escape the Git SHA-1 checksum parameters provided to commit notifications when displaying them in a build cause, resulting in a stored cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2021-21684**	https://www.jenkins.io/security/advisory/2021-10-06/#SECURITY-2499	A-JEN-GIT-201021/227
Johnsoncontrols					
exacqvision_server					
Integer Overflow or Wraparound	11-Oct-21	5	An unauthenticated remote user could exploit a potential integer overflow condition in the exacqVision Server with a	https://www.johnsoncontrols.com/cyber-solutions/sec	A-JOH-EXAC-201021/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted script and cause denial-of-service condition. **CVE ID : CVE-2021-27665**	urity-advisories	
justwriting_project					
justwriting					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in application/controllers/dropbox.php in JustWriting 1.0.0 and below allow remote attackers to inject arbitrary web script or HTML via the challenge parameter. **CVE ID : CVE-2021-41467**	N/A	A-JUS-JUST-201021/229
Kibokolabs					
chained_quiz					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-21	3.5	The Chained Quiz WordPress plugin before 1.2.7.2 does not properly sanitize or escape inputs in the plugin's settings. **CVE ID : CVE-2021-24690**	N/A	A-KIB-CHAI-201021/230
Kriesi					
enfold					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-21	4.3	The Enfold Enfold WordPress theme before 4.8.4 was vulnerable to Reflected Cross-Site Scripting (XSS). The vulnerability is present on Enfold versions previous than 4.8.4 which use Avia Page Builder.	N/A	A-KRI-ENFO-201021/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24719		
laquisscada					
scada					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Oct-21	6.8	LCDS LAquis SCADA through 4.3.1.1085 is vulnerable to a control bypass and path traversal. If an attacker can get a victim to load a malicious els project file and use the play feature, then the attacker can bypass a consent popup and write arbitrary files to OS locations where the user has permission, leading to code execution. **CVE ID : CVE-2021-41579**	N/A	A-LAQ-SCAD-201021/232
lightning_network_daemon_project					
lightning_network_daemon					
Incorrect Authorization	04-Oct-21	7.5	Lightning Labs lnd before 0.13.3-beta allows loss of funds because of dust HTLC exposure. **CVE ID : CVE-2021-41593**	https://lists.linuxfoundation.org/pipermail/lightning-dev/2020-May/002714.html, https://lists.linuxfoundation.org/pipermail/lightning-dev/2021-October/003257.html, https://lists.linuxfoundation.org/pipermail/lightning-dev/2021-	A-LIG-LIGH-201021/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				October/003264.html	
Linuxfoundation					
containerd					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Oct-21	7.2	containerd is an open source container runtime with an emphasis on simplicity, robustness and portability. A bug was found in containerd where container root directories and some plugins had insufficiently restricted permissions, allowing otherwise unprivileged Linux users to traverse directory contents and execute programs. When containers included executable programs with extended permission bits (such as setuid), unprivileged Linux users could discover and execute those programs. When the UID of an unprivileged Linux user on the host collided with the file owner or group inside a container, the unprivileged Linux user on the host could discover, read, and modify those files. This vulnerability has been fixed in containerd 1.4.11 and containerd 1.5.7. Users should update to these version when they are released and may restart containers or update directory	https://github.com/containerd/containerd/commit/5b46e404f6b9f661a205e28d59c982d3634148f8, https://github.com/containerd/containerd/security/advisories/GHSA-c2h3-6mxw-7mvq	A-LIN-CONT-201021/234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permissions to mitigate the vulnerability. Users unable to update should limit access to the host to trusted users. Update directory permission on container bundles directories. **CVE ID : CVE-2021-41103**		
lodging_reservation_management_system_project					
lodging_reservation_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Oct-21	7.5	The username and password field of login in Lodging Reservation Management System V1 can give access to any user by using SQL injection to bypass authentication. **CVE ID : CVE-2021-41511**	N/A	A-LOD-LODG-201021/235
Maianscriptworld					
maian_cart					
Missing Authorization	07-Oct-21	7.5	Maian Cart v3.8 contains a preauthorization remote code execution (RCE) exploit via a broken access control issue in the Elfinder plugin. **CVE ID : CVE-2021-32172**	https://www.maianscriptworld.co.uk/	A-MAI-MAIA-201021/236
Mcafee					
drive_encryption					
Improper Privilege Management	01-Oct-21	4.6	Privilege Escalation vulnerability in a Windows system driver of McAfee Drive Encryption (DE) prior to 7.3.0 could allow a local non-admin user to	https://kc.mcafee.com/corporate/index?page=content&id=SB10361	A-MCA-DRIV-201021/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			gain elevated system privileges via exploiting an unutilized memory buffer. **CVE ID : CVE-2021-23893**		
Mediawiki					
mediawiki					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-21	4.3	MediaWiki before 1.36.2 allows XSS. Month related MediaWiki messages are not escaped before being used on the Special:Search results page. **CVE ID : CVE-2021-41798**	https://phabricator.wikimedia.org/T285515	A-MED-MEDI-201021/238
Loop with Unreachable Exit Condition ('Infinite Loop')	06-Oct-21	5	An issue was discovered in MediaWiki through 1.36.2. A parser function related to loop control allowed for an infinite loop (and php-fpm hang) within the Loops extension because egLoopsCountLimit is mishandled. This could lead to memory exhaustion. **CVE ID : CVE-2021-42040**	https://gerrit.wikimedia.org/r/q/I0caf6f129f94612b5bcf406a171aa5ffedea1f80, https://phabricator.wikimedia.org/T287347	A-MED-MEDI-201021/239
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-21	4.3	An issue was discovered in CentralAuth in MediaWiki through 1.36.2. The rightsnone MediaWiki message was not being properly sanitized and allowed for the injection and execution of HTML and JavaScript via the setchange log. **CVE ID : CVE-2021-42041**	https://phabricator.wikimedia.org/T291696, https://gerrit.wikimedia.org/r/q/I7aeaa6e4de5ccaa5eeb6bf4fb00c96b01d5fea35	A-MED-MEDI-201021/240
Improper Neutralizatio	06-Oct-21	3.5	An issue was discovered in SpecialEditGrowthConfig in	https://phabricator.wikime	A-MED-MEDI-201021/241

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 of Input During Web Page Generation ('Cross-site Scripting')			the GrowthExperiments extension in MediaWiki through 1.36.2. The growthexperiments-edit-config-error-invalid-title MediaWiki message was not being properly sanitized and allowed for the injection and execution of HTML and JavaScript. **CVE ID : CVE-2021-42042**	dia.org/T290692, https://gerrit.wikimedia.org/r/q/Ibeb13d032ca044af53f6b2334e27b6b97b6f4e9f	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-21	4.3	An issue was discovered in Special:MediaSearch in the MediaSearch extension in MediaWiki through 1.36.2. The suggestion text (a parameter to mediasearch-did-you-mean) was not being properly sanitized and allowed for the injection and execution of HTML and JavaScript via the intitle: search operator within the query. **CVE ID : CVE-2021-42043**	https://gerrit.wikimedia.org/r/q/If64eb5842237c92290d07ebc3fe14710d9de3fc2, https://phabricator.wikimedia.org/T291600	A-MED-MEDI-201021/242
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-21	3.5	An issue was discovered in the Mentor dashboard in the GrowthExperiments extension in MediaWiki through 1.36.2. The Growthexperiments-mentor-dashboard-mentee-overview-add-filter-total-edits-headline, growthexperiments-mentor-dashboard-mentee-overview-add-filter-starred-headline, growthexperiments-mentor-dashboard-	https://phabricator.wikimedia.org/T289408, https://gerrit.wikimedia.org/r/q/I858d55fb2eca9b50ac6ef5a6f2a7b2784f0fa0d6	A-MED-MEDI-201021/243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mentee-overview-info-text, growthexperiments-mentor-dashboard-mentee-overview-info-legend-headline, and growthexperiments-mentor-dashboard-mentee-overview-active-ago MediaWiki messages were not being properly sanitized and allowed for the injection and execution of HTML and JavaScript. **CVE ID : CVE-2021-42044**		
meowapps					
media_file_renamer_-_auto_\\&_manual_rename					
Cross-Site Request Forgery (CSRF)	04-Oct-21	4.3	Cross-Site Request Forgery (CSRF) vulnerability in WordPress Media File Renamer – Auto & Manual Rename plugin (versions <= 5.1.9). Affected parameters "post_title", "filename", "lock". This allows changing the uploaded media title, media file name, and media locking state. **CVE ID : CVE-2021-36850**	https://wordpress.org/plugins/media-file-renamer/#developers	A-MEO-MEDI-201021/244
meow_gallery					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	04-Oct-21	5.5	The Meow Gallery WordPress plugin before 4.1.9 does not sanitise, validate or escape the ids attribute of its gallery shortcode (available for users as low as Contributor) before using it in an SQL statement,	N/A	A-MEO-MEOW-201021/245

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
Injection')			leading to an authenticated SQL Injection issue. The injection also allows the returned values to be manipulated in a way that could lead to data disclosure and arbitrary objects to be deserialized. **CVE ID : CVE-2021-24465**		
micron					
ballistix_memory_overview_display_utility					
Improper Privilege Management	04-Oct-21	7.2	Ballistix MOD Utility through 2.0.2.5 is vulnerable to privilege escalation in the MODAPI.sys driver component. The vulnerability is triggered by sending a specific IOCTL request that allows low-privileged users to directly interact with physical memory via the MmMapIoSpace function call (mapping physical memory into a virtual address space). Attackers could exploit this issue to achieve local privilege escalation to NT AUTHORITY\SYSTEM. **CVE ID : CVE-2021-41285**	N/A	A-MIC-BALL-201021/246
mkdocs					
mkdocs					
Improper Limitation of a Pathname to a	07-Oct-21	5	** DISPUTED ** The mkdocs 1.2.2 built-in dev-server allows directory traversal using the port	N/A	A-MKD-MKDO-201021/247

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
Restricted Directory ('Path Traversal')			8000, enabling remote exploitation to obtain :sensitive information. NOTE: the vendor has disputed this as described in https://github.com/mkdocs/mkdocs/issues/2601.] and https://github.com/nisdn/CVE-2021-40978/issues/1. **CVE ID : CVE-2021-40978**		
mobyproject					
moby					
Improper Preservation of Permissions	04-Oct-21	4.4	Moby is an open-source project created by Docker to enable software containerization. A bug was found in Moby (Docker Engine) where attempting to copy files using `docker cp` into a specially-crafted container can result in Unix file permission changes for existing files in the hostâ€™s filesystem, widening access to others. This bug does not directly allow files to be read, modified, or executed without an additional cooperating process. This bug has been fixed in Moby (Docker Engine) 20.10.9. Users should update to this version as soon as possible. Running containers do not need to be restarted. **CVE ID : CVE-2021-41089**	https://github.com/moby/moby/commit/bce32e5c93be4caf1a592582155b9cb837fc129a, https://github.com/moby/moby/security/advisories/GHSA-v994-f8vw-g7j4	A-MOB-MOBY-201021/248

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 Preservation of Permissions	04-Oct-21	4.6	Moby is an open-source project created by Docker to enable software containerization. A bug was found in Moby (Docker Engine) where the data directory (typically `/var/lib/docker`) contained subdirectories with insufficiently restricted permissions, allowing otherwise unprivileged Linux users to traverse directory contents and execute programs. When containers included executable programs with extended permission bits (such as `setuid`), unprivileged Linux users could discover and execute those programs. When the UID of an unprivileged Linux user on the host collided with the file owner or group inside a container, the unprivileged Linux user on the host could discover, read, and modify those files. This bug has been fixed in Moby (Docker Engine) 20.10.9. Users should update to this version as soon as possible. Running containers should be stopped and restarted for the permissions to be fixed. For users unable to upgrade limit access to the host to trusted users. Limit access to host volumes to	https://github.com/moby/moby/commit/f0ab919f518c47240ea0e72d0999576bb8008e64, https://github.com/moby/moby/security/advisories/GHSA-3fwx-pjgw-3558	A-MOB-MOBY-201021/249

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
			trusted containers. **CVE ID : CVE-2021-41091**		
myscada					
mydesigner					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Oct-21	6.8	mySCADA myDESIGNER 8.20.0 and below allows Directory Traversal attacks when importing project files. If an attacker can trick a victim into importing a malicious mep file, then they gain the ability to write arbitrary files to OS locations where the user has permission. This would typically lead to code execution. **CVE ID : CVE-2021-41578**	N/A	A-MYS-MYDE-201021/250
mysurvey					
survey_solutions					
Exposure of Sensitive Information to an Unauthorized Actor	04-Oct-21	5	Survey Solutions is a survey management and data collection system. In affected versions the Headquarters application publishes /metrics endpoint available to any user. None of the survey answers are ever exposed, only the aggregate counters, including count of interviews, or count of assignments. Starting from version 21.09.1 the endpoint is turned off by default. **CVE ID : CVE-2021-41123**	https://github.com/surveysolutions/surveysolutions/commit/99e7e8345cb98f2eda08e37976e3d3aeb49971c9, https://github.com/surveysolutions/surveysolutions/security/advisories/GHSA-6c7j-7jf3-9p3j	A-MYS-SURV-201021/251
Nagios					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nagios_xi					
Server-Side Request Forgery (SSRF)	05-Oct-21	4	Nagios Enterprises NagiosXI <= 5.8.4 contains a Server-Side Request Forgery (SSRF) vulnerability in schedulereport.php. Any authenticated user can create scheduled reports containing PDF screenshots of any view in the NagiosXI application. Due to lack of input sanitisation, the target page can be replaced with an SSRF payload to access internal resources or disclose local system files. **CVE ID : CVE-2021-37223**	http://nagios.com, https://www.nagios.com/downloads/nagios-xi/changelog/	A-NAG-NAGI-201021/252
Netsarang					
xshell					
N/A	07-Oct-21	5	Xshell before 7.0.0.76 allows attackers to cause a crash by triggering rapid changes to the title bar. **CVE ID : CVE-2021-42095**	https://www.netsarang.com/en/xshell-update-history/	A-NET-XSHE-201021/253
Nodejs					
node.js					
Use After Free	07-Oct-21	5	Node.js before 16.6.0, 14.17.4, and 12.22.4 is vulnerable to a use after free attack where an attacker might be able to exploit the memory corruption, to change process behavior. **CVE ID : CVE-2021-22930**	https://nodejs.org/en/blog/vulnerability/july-2021-security-releases-2/	A-NOD-NODE-201021/254

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
Octobercms					
october					
Improper Authentication	06-Oct-21	6.5	October is a Content Management System (CMS) and web platform built on the the Laravel PHP Framework. In affected versions administrator accounts which had previously been deleted may still be able to sign in to the backend using October CMS v2.0. The issue has been patched in v2.1.12 of the october/october package. There are no workarounds for this issue and all users should update. **CVE ID : CVE-2021-41126**	https://github.com/octobercms/october/security/advisories/GHSA-6gjf-7w99-j7x7, https://octobercms.com/changelog	A-OCT-OCTO-201021/255
octopus					
octopus_deploy					
Untrusted Search Path	07-Oct-21	4.4	When Octopus Server is installed using a custom folder location, folder ACLs are not set correctly and could lead to an unprivileged user using DLL side-loading to gain privileged access. **CVE ID : CVE-2021-26556**	https://advisories.octopus.com/adv/2021-01---Local-privilege-escalation-in-Octopus-Server-(CVE-2021-26556).1733296189.html	A-OCT-OCTO-201021/256
tentacle					
Untrusted Search Path	07-Oct-21	4.4	When Octopus Tentacle is installed using a custom folder location, folder ACLs are not set correctly and	https://advisories.octopus.com/adv/2021-02---Local-	A-OCT-TENT-201021/257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could lead to an unprivileged user using DLL side-loading to gain privileged access. **CVE ID : CVE-2021-26557**	privilege-escalation-in-Octopus-Tentacle-(CVE-2021-26557).1732870264.html	
omikron					
multicash					
Improper Authentication	05-Oct-21	4.6	Omikron MultiCash Desktop 4.00.008.SP5 relies on a client-side authentication mechanism. When a user logs into the application, the validity of the password is checked locally. All communication to the database backend is made via the same technical account. Consequently, an attacker can attach a debugger to the process or create a patch that manipulates the behavior of the login function. When the function always returns the success value (corresponding to a correct password), an attacker can login with any desired account, such as the administrative account of the application. **CVE ID : CVE-2021-41286**	N/A	A-OMI-MULT-201021/258
Onionshare					
onionshare					
N/A	04-Oct-21	5	An information disclosure vulnerability in OnionShare	https://github.com/onions	A-ONI-ONIO-

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
			2.3 before 2.4 allows remote unauthenticated attackers to retrieve the full list of participants of a non-public OnionShare node via the --chat feature. **CVE ID : CVE-2021-41867**	hare/onionshare/compare/v2.3.3...v2.4	201021/259
N/A	04-Oct-21	7.5	OnionShare 2.3 before 2.4 allows remote unauthenticated attackers to upload files on a non-public node when using the --receive functionality. **CVE ID : CVE-2021-41868**	https://github.com/onionshare/onionshare/compare/v2.3.3...v2.4	A-ONI-ONIO-201021/260
online-shopping-system-advanced_project					
online-shopping-system-advanced					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Oct-21	5	An un-authenticated SQL Injection exists in PuneethReddyHC online-shopping-system-advanced through the /action.php prId parameter. Using a post request does not sanitize the user input. **CVE ID : CVE-2021-41648**	N/A	A-ONL-ONLI-201021/261
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Oct-21	7.5	An un-authenticated SQL Injection exists in PuneethReddyHC online-shopping-system-advanced through the /homeaction.php cat_id parameter. Using a post request does not sanitize the user input. **CVE ID : CVE-2021-41649**	N/A	A-ONL-ONLI-201021/262
online_food_ordering_web_app_project					
online_food_ordering_web_app					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Oct-21	6.4	An un-authenticated error-based and time-based blind SQL injection vulnerability exists in Kaushik Jadhav Online Food Ordering Web App 1.0. An attacker can exploit the vulnerable "username" parameter in login.php and retrieve sensitive database information, as well as add an administrative user. **CVE ID : CVE-2021-41647**	N/A	A-ONL-ONLI-201021/263
open5gs					
open5gs					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-21	5	ogs_fqdn_parse in Open5GS 1.0.0 through 2.3.3 inappropriately trusts a client-supplied length value, leading to a buffer overflow. The attacker can send a PFCP Session Establishment Request with "internet" as the PDI Network Instance. The first character is interpreted as a length value to be used in a memcpy call. The destination buffer is only 100 bytes long on the stack. Then, 'i' gets interpreted as 105 bytes to copy from the source buffer to the destination buffer. **CVE ID : CVE-2021-41794**	N/A	A-OPE-OPEN-201021/264
openwaygroup					
way4					
Improper	11-Oct-21	4.3	OpenWay WAY4 ACS	https://www.	A-OPE-WAY4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			before 1.2.278-2693 allows XSS via the /way4acs/enroll action parameter. **CVE ID : CVE-2021-35059**	openwaygroup.com/way4-platform	201021/265
Oracle					
openjdk					
Improper Privilege Management	06-Oct-21	4.6	An insecure modification flaw in the /etc/passwd file was found in the openjdk-1.8 and openjdk-11 containers. This flaw allows an attacker with access to the container to modify the /etc/passwd and escalate their privileges. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2021-20264**	N/A	A-ORA-OPEN-201021/266
pardus					
liderahenk					
Missing Authentication for Critical Function	01-Oct-21	5	On 2.1.15 version and below of Lider module in LiderAhenk software is leaking it's configurations via an unsecured API. An attacker with an access to the configurations API could get valid LDAP credentials. **CVE ID : CVE-2021-3825**	https://www.usom.gov.tr/bildirim/tr-21-0795, https://pentest.blog/liderahenk-0day-all-your-pardus-clients-belongs-to-me/	A-PAR-LIDE-201021/267
paymentplugins					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
stripe_for_woocommerce					
Missing Authorization	04-Oct-21	4	The Stripe for WooCommerce WordPress plugin is missing a capability check on the save() function found in the ~/includes/admin/class-wc-stripe-admin-user-edit.php file that makes it possible for attackers to configure their account to use other site users unique STRIPE identifier and make purchases with their payment accounts. This affects versions 3.0.0 - 3.3.9. **CVE ID : CVE-2021-39347**	https://plugins.trac.wordpress.org/changeset/2601162/woo-stripe-payment/trunk/includes/admin/class-wc-stripe-admin-user-edit.php	A-PAY-STRI-201021/268
PHP					
php					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Oct-21	4.3	In PHP versions 7.3.x below 7.3.29, 7.4.x below 7.4.21 and 8.0.x below 8.0.8, when using Firebird PDO driver extension, a malicious database server could cause crashes in various database functions, such as getAttribute(), execute(), fetch() and others by returning invalid response data that is not parsed correctly by the driver. This can result in crashes, denial of service or potentially memory corruption. **CVE ID : CVE-2021-21704**	https://bugs.php.net/bug.php?id=76450, https://bugs.php.net/bug.php?id=76452, https://bugs.php.net/bug.php?id=76449, https://bugs.php.net/bug.php?id=76448	A-PHP-PHP-201021/269
Improper Input	04-Oct-21	5	In PHP versions 7.3.x below 7.3.29, 7.4.x below 7.4.21	https://bugs.php.net/bug.p	A-PHP-PHP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			and 8.0.x below 8.0.8, when using URL validation functionality via filter_var() function with FILTER_VALIDATE_URL parameter, an URL with invalid password field can be accepted as valid. This can lead to the code incorrectly parsing the URL and potentially leading to other security implications - like contacting a wrong server or making a wrong access decision. **CVE ID : CVE-2021-21705**	hp?id=81122	201021/270
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Oct-21	4.3	In PHP versions 7.3.x below 7.3.31, 7.4.x below 7.4.24 and 8.0.x below 8.0.11, in Microsoft Windows environment, ZipArchive::extractTo may be tricked into writing a file outside target directory when extracting a ZIP file, thus potentially causing files to be created or overwritten, subject to OS permissions. **CVE ID : CVE-2021-21706**	https://bugs.php.net/bug.php?id=81420	A-PHP-PHP-201021/271
Php-fusion					
phpfusion					
Improper Neutralization of Input During Web Page Generation ('Cross-site	11-Oct-21	4.3	PHPFusion 9.03.110 is affected by cross-site scripting (XSS) in the preg patterns filter html tag without "//" in descript() function An authenticated user can trigger XSS by	N/A	A-PHP-PHPF-201021/272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			appending "//" in the end of text. **CVE ID : CVE-2021-40541**		
Pingidentity					
pingfederate					
Improper Restriction of XML External Entity Reference	07-Oct-21	5	Ping Identity PingFederate before 10.3.1 mishandles pre-parsing validation, leading to an XXE attack that can achieve XML file disclosure. **CVE ID : CVE-2021-41770**	https://docs.pingidentity.com/bundle/pingfederate-103/page/ruz1628492711606.html, https://www.pingidentity.com/en/resources/downloads/pingfederate.html	A-PIN-PING-201021/273
pixeline					
bugs					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in install/index.php in bugs 1.8 and below version allows remote attackers to inject arbitrary web script or HTML via the last_name parameter. **CVE ID : CVE-2021-40922**	N/A	A-PIX-BUGS-201021/274
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in install/index.php in bugs 1.8 and below version allows remote attackers to inject arbitrary web script or HTML via the email parameter. **CVE ID : CVE-2021-40923**	N/A	A-PIX-BUGS-201021/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in install/index.php in bugs 1.8 and below version allows remote attackers to inject arbitrary web script or HTML via the first_name parameter. **CVE ID : CVE-2021-40924**	N/A	A-PIX-BUGS-201021/276
Postgresql					
postgresql					
N/A	08-Oct-21	4	A flaw was found in postgresql. Using an UPDATE ... RETURNING command on a purpose-crafted table, an authenticated database user could read arbitrary bytes of server memory. The highest threat from this vulnerability is to data confidentiality. **CVE ID : CVE-2021-32029**	https://www.postgresql.org/support/security/CVE-2021-32029/, https://bugzilla.redhat.com/show_bug.cgi?id=1956883	A-POS-POST-201021/277
Projectsend					
projectsend					
Incorrect Authorization	11-Oct-21	5.5	Projectsend version r1295 is affected by sensitive information disclosure. Because of not checking authorization in ids parameter in files-edit.php and id parameter in process.php function, a user with uploader role can download and edit all files of users in application. **CVE ID : CVE-2021-40884**	N/A	A-PRO-PROJ-201021/278
Improper	11-Oct-21	4	Projectsend version r1295	N/A	A-PRO-PROJ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			is affected by a directory traversal vulnerability. A user with Uploader role can add value `2` for `chunks` parameter to bypass `fileName` sanitization. **CVE ID : CVE-2021-40886**		201021/279
Qnap					
image2pdf					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	3.5	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Image2PDF. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Image2PDF: Image2PDF 2.1.5 (2021/08/17) and later **CVE ID : CVE-2021-38675**	https://www.qnap.com/en/security-advisory/qsa-21-43	A-QNA-IMAG-201021/280
photo_station					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	3.5	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Photo Station. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Photo Station: Photo Station 6.0.18 (2021/09/01) and	https://www.qnap.com/en/security-advisory/qsa-21-41	A-QNA-PHOT-201021/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			later **CVE ID : CVE-2021-34354**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	3.5	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP NAS running Photo Station. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Photo Station: Photo Station 5.4.10 (2021/08/19) and later Photo Station 5.7.13 (2021/08/19) and later Photo Station 6.0.18 (2021/09/01) and later **CVE ID : CVE-2021-34355**	https://www.qnap.com/en/security-advisory/qsa-21-42	A-QNA-PHOT-201021/282
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	3.5	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Photo Station. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Photo Station: Photo Station 6.0.18 (2021/09/01) and later **CVE ID : CVE-2021-34356**	https://www.qnap.com/en/security-advisory/qsa-21-41	A-QNA-PHOT-201021/283
qvr					
Improper Neutralization of Special	01-Oct-21	7.5	A command injection vulnerability has been reported to affect QNAP	https://www.qnap.com/en/security-	A-QNA-QVR-201021/284

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
Elements used in a Command ('Command Injection')			device running QVR. If exploited, this vulnerability could allow remote attackers to run arbitrary commands. We have already fixed this vulnerability in the following versions of QVR: QVR 5.1.5 build 20210902 and later **CVE ID : CVE-2021-34352**	advisory/qsa-21-38	
rconfig					
rconfig					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Oct-21	6.5	rConfig 3.9.6 is affected by SQL Injection. A user must be authenticated to exploit the vulnerability. If --secure-file-priv in MySQL server is not set and the Mysql server is the same as rConfig, an attacker may successfully upload a webshell to the server and access it remotely. **CVE ID : CVE-2021-29004**	https://rconfig.com, http://rconfig.com	A-RCO-RCON-201021/285
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-21	4	rConfig 3.9.6 is affected by a Local File Disclosure vulnerability. An authenticated user may successfully download any file on the server. **CVE ID : CVE-2021-29006**	http://rconfig.com	A-RCO-RCON-201021/286
Redhat					
jboss_enterprise_application_platform					
N/A	08-Oct-21	4	A flaw was found in postgresql. Using an UPDATE ... RETURNING command on a purpose-	https://www.postgresql.org/support/security/CVE-	A-RED-JBOS-201021/287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted table, an authenticated database user could read arbitrary bytes of server memory. The highest threat from this vulnerability is to data confidentiality. **CVE ID : CVE-2021-32029**	2021-32029/, https://bugzilla.redhat.com/show_bug.cgi?id=1956883	
openshift					
N/A	08-Oct-21	1.9	IBM App Connect Enterprise Certified Container 1.0, 1.1, 1.2, 1.3, 1.4 and 1.5 could disclose sensitive information to a local user when it is configured to use an IBM Cloud API key to connect to cloud-based connectors. IBM X-Force ID: 207630. **CVE ID : CVE-2021-29906**	https://www.ibm.com/support/pages/node/6497177, https://exchange.xforce.ibmcloud.com/vulnerabilities/207630	A-RED-OPEN-201021/288
software_collections					
Out-of-bounds Read	04-Oct-21	4	Redis is an open source, in-memory database that persists on disk. When using the Redis Lua Debugger, users can send malformed requests that cause the debugger's protocol parser to read data beyond the actual buffer. This issue affects all versions of Redis with Lua debugging support (3.2 or newer). The problem is fixed in versions 6.2.6, 6.0.16 and 5.0.14. **CVE ID : CVE-2021-32672**	https://github.com/redis/redis/security/advisories/GHSA-9mj9-xx53-qmxm, https://github.com/redis/redis/commit/6ac3c0b7abd35f37201ed2d6298ecef4ea1ae1dd	A-RED-SOFT-201021/289
redis					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
hiredis					
Integer Overflow or Wraparound	04-Oct-21	6.5	Hiredis is a minimalistic C client library for the Redis database. In affected versions Hiredis is vulnurable to integer overflow if provided maliciously crafted or corrupted `RESP` `mult-bulk` protocol data. When parsing `multi-bulk` (array-like) replies, hiredis fails to check if `count * sizeof(redisReply*)` can be represented in `SIZE_MAX`. If it can not, and the `calloc()` call doesn't itself make this check, it would result in a short allocation and subsequent buffer overflow. Users of hiredis who are unable to update may set the [maxelements](https://github.com/redis/hiredis#reader-max-array-elements) context option to a value small enough that no overflow is possible. **CVE ID : CVE-2021-32765**	https://github.com/redis/hiredis/security/advisories/GHSA-hfm9-39pp-55p2, https://github.com/redis/hiredis/commit/76a7b10005c70babee357a7d0f2becf28ec7ed1e	A-RED-HIRE-201021/290
redis					
Integer Overflow or Wraparound	04-Oct-21	6	Redis is an open source, in-memory database that persists on disk. An integer overflow bug in the underlying string library can be used to corrupt the heap and potentially result with denial of service or remote code execution. The	https://github.com/redis/redis/commit/c6ad876774f3cc11e32681ea02a2eead00f2c521, https://github.com/redis/r	A-RED-REDI-201021/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability involves changing the default proto-max-bulk-len configuration parameter to a very large value and constructing specially crafted network payloads or commands. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the proto-max-bulk-len configuration parameter. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command. **CVE ID : CVE-2021-41099**	edis/security/advisories/GHSA-j3cr-9h5g-6cph	
Out-of-bounds Write	04-Oct-21	6.5	Redis is an open source, in-memory database that persists on disk. In affected versions specially crafted Lua scripts executing in Redis can cause the heap-based Lua stack to be overflowed, due to incomplete checks for this condition. This can result with heap corruption and potentially remote code execution. This problem exists in all versions of Redis with Lua scripting support, starting from 2.6. The problem is fixed in versions 6.2.6, 6.0.16 and	https://github.com/redis/redis/commit/666ed7facf4524bf6d19b11b20faa2cf93fdf591, https://github.com/redis/redis/security/advisories/GHSA-p486-xggp-782c	A-RED-REDI-201021/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.0.14. For users unable to update an additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from executing Lua scripts. This can be done using ACL to restrict EVAL and EVALSHA commands. **CVE ID : CVE-2021-32626**		
Integer Overflow or Wraparound	04-Oct-21	6	Redis is an open source, in-memory database that persists on disk. In affected versions an integer overflow bug in Redis can be exploited to corrupt the heap and potentially result with remote code execution. The vulnerability involves changing the default proto-max-bulk-len and client-query-buffer-limit configuration parameters to very large values and constructing specially crafted very large stream elements. The problem is fixed in Redis 6.2.6, 6.0.16 and 5.0.14. For users unable to upgrade an additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the proto-max-bulk-len configuration parameter. This can be	https://github.com/redis/redis/commit/f6a40570fa63d5afdd596c78083d754081d80ae3, https://github.com/redis/redis/security/advisories/GHSA-f434-69fm-g45v	A-RED-REDI-201021/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			done using ACL to restrict unprivileged users from using the CONFIG SET command. **CVE ID : CVE-2021-32627**		
Integer Overflow or Wraparound	04-Oct-21	6	Redis is an open source, in-memory database that persists on disk. An integer overflow bug in the ziplist data structure used by all versions of Redis can be exploited to corrupt the heap and potentially result with remote code execution. The vulnerability involves modifying the default ziplist configuration parameters (hash-max-ziplist-entries, hash-max-ziplist-value, zset-max-ziplist-entries or zset-max-ziplist-value) to a very large value, and then constructing specially crafted commands to create very large ziplists. The problem is fixed in Redis versions 6.2.6, 6.0.16, 5.0.14. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the above configuration parameters. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command.	https://github.com/redis/redis/commit/f6a40570fa63d5afdd596c78083d754081d80ae3, https://github.com/redis/redis/security/advisories/GHSA-vw22-qm3h-49pr	A-RED-REDI-201021/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-32628		
Allocation of Resources Without Limits or Throttling	04-Oct-21	5	Redis is an open source, in-memory database that persists on disk. When parsing an incoming Redis Standard Protocol (RESP) request, Redis allocates memory according to user-specified values which determine the number of elements (in the multi-bulk header) and size of each element (in the bulk header). An attacker delivering specially crafted requests over multiple connections can cause the server to allocate significant amount of memory. Because the same parsing mechanism is used to handle authentication requests, this vulnerability can also be exploited by unauthenticated users. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. An additional workaround to mitigate this problem without patching the redis-server executable is to block access to prevent unauthenticated users from connecting to Redis. This can be done in different ways: Using network access control tools like firewalls, iptables, security groups, etc. or Enabling TLS and requiring users to	https://github.com/redis/redis/commit/5674b0057ff2903d43eaff802017eddf37c360f8, https://github.com/redis/redis/security/advisories/GHSA-f6pw-v9gw-v64p	A-RED-REDI-201021/295

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
			authenticate using client side certificates. **CVE ID : CVE-2021-32675**		
Integer Overflow or Wraparound	04-Oct-21	6	Redis is an open source, in-memory database that persists on disk. An integer overflow bug affecting all versions of Redis can be exploited to corrupt the heap and potentially be used to leak arbitrary contents of the heap or trigger remote code execution. The vulnerability involves changing the default set-max-intset-entries configuration parameter to a very large value and constructing specially crafted commands to manipulate sets. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the set-max-intset-entries configuration parameter. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command. **CVE ID : CVE-2021-32687**	https://github.com/redis/redis/security/advisories/GHSA-m3mf-8x9w-r27q, https://github.com/redis/redis/commit/a30d367a71b7017581cf1ca104242a3c644dec0f	A-RED-REDI-201021/296
Integer Overflow or Wraparound	04-Oct-21	9	Redis is an open source, in-memory database that persists on disk. The redis-	https://github.com/redis/redis/security/	A-RED-REDI-201021/297

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
			cli command line tool and redis-sentinel service may be vulnerable to integer overflow when parsing specially crafted large multi-bulk network replies. This is a result of a vulnerability in the underlying hiredis library which does not perform an overflow check before calling the calloc() heap allocation function. This issue only impacts systems with heap allocators that do not perform their own overflow checks. Most modern systems do and are therefore not likely to be affected. Furthermore, by default redis-sentinel uses the jemalloc allocator which is also not vulnerable. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. **CVE ID : CVE-2021-32762**	advisories/GHSA-833w-8v3m-8wwr, https://github.com/redis/redis/commit/0215324a66af949be39b34be2d55143232c1cb71	
redislabs					
redis					
Out-of-bounds Read	04-Oct-21	4	Redis is an open source, in-memory database that persists on disk. When using the Redis Lua Debugger, users can send malformed requests that cause the debugger's protocol parser to read data beyond the actual buffer. This issue affects all versions of Redis with Lua	https://github.com/redis/redis/security/advisories/GHSA-9mj9-xx53-qmxm, https://github.com/redis/redis/commit/6ac3c0b7abd35f37201ed2	A-RED-REDI-201021/298

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
			debugging support (3.2 or newer). The problem is fixed in versions 6.2.6, 6.0.16 and 5.0.14. **CVE ID : CVE-2021-32672**	d6298ecef4ea1ae1dd	
salesagility					
suitecrm					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Oct-21	5	SuiteCRM before 7.10.33 and 7.11.22 allows information disclosure via Directory Traversal. An attacker can partially include arbitrary files via the file_name parameter of the Step3 import functionality. **CVE ID : CVE-2021-41595**	https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_22, https://docs.suitecrm.com/admin/releases/7.10.x/#_7_10_33	A-SAL-SUIT-201021/299
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Oct-21	5	SuiteCRM before 7.10.33 and 7.11.22 allows information disclosure via Directory Traversal. An attacker can partially include arbitrary files via the importFile parameter of the RefreshMapping import functionality. **CVE ID : CVE-2021-41596**	https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_22, https://docs.suitecrm.com/admin/releases/7.10.x/#_7_10_33, https://suitecrm.com	A-SAL-SUIT-201021/300
Improper Privilege Management	04-Oct-21	6.5	SuiteCRM 7.10.x before 7.10.33 and 7.11.x before 7.11.22 is vulnerable to privilege escalation. **CVE ID : CVE-2021-41869**	https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_22, https://docs.suitecrm.com/admin/releases/7.10.x/#_7_10_33,	A-SAL-SUIT-201021/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://suitecrm.com	
Samsung					
galaxy_store					
N/A	06-Oct-21	2.1	Intent redirection vulnerability in SamsungAccountSDKSigninActivity of Galaxy Store prior to version 4.5.32.4 allows attacker to access content provider of Galaxy Store. **CVE ID : CVE-2021-25499**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=10	A-SAM-GALA-201021/302
notes					
Out-of-bounds Write	06-Oct-21	3.6	Lack of boundary checking of a buffer in libSPenBase library of Samsung Notes prior to Samsung Note version 4.3.02.61 allows OOB read. **CVE ID : CVE-2021-25492**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=10	A-SAM-NOTE-201021/303
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Oct-21	3.6	Lack of boundary checking of a buffer in libSPenBase library of Samsung Notes prior to Samsung Note version 4.3.02.61 allows OOB read **CVE ID : CVE-2021-25493**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=10	A-SAM-NOTE-201021/304
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	4.6	A possible buffer overflow vulnerability in libSPenBase library of Samsung Notes prior to Samsung Note version 4.3.02.61 allows arbitrary code execution. **CVE ID : CVE-2021-25494**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=10	A-SAM-NOTE-201021/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Oct-21	4.6	A possible heap buffer overflow vulnerability in libSPenBase library of Samsung Notes prior to Samsung Note version 4.3.02.61 allows arbitrary code execution. **CVE ID : CVE-2021-25495**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=10	A-SAM-NOTE-201021/306
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	4.6	A possible buffer overflow vulnerability in maetd_dec_slice of libSPenBase library of Samsung Notes prior to Samsung Notes version 4.3.02.61 allows arbitrary code execution. **CVE ID : CVE-2021-25496**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=10	A-SAM-NOTE-201021/307
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	4.6	A possible buffer overflow vulnerability in maetd_cpy_slice of libSPenBase library of Samsung Notes prior to Samsung Notes version 4.3.02.61 allows arbitrary code execution. **CVE ID : CVE-2021-25497**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=10	A-SAM-NOTE-201021/308
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	4.6	A possible buffer overflow vulnerability in maetd_eco_cb_mode of libSPenBase library of Samsung Notes prior to Samsung Notes version 4.3.02.61 allows arbitrary code execution. **CVE ID : CVE-2021-25498**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=10	A-SAM-NOTE-201021/309
scalabium					
dbase_viewer					
Buffer Copy	01-Oct-21	6.8	Scalabium dBase Viewer	N/A	A-SCA-DBAS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			version 2.6 (Build 5.751) is vulnerable to remote code execution via a crafted DBF file that triggers a buffer overflow. An attacker can use the Structured Exception Handler (SEH) records and redirect execution to attacker-controlled code. **CVE ID : CVE-2021-35297**		201021/310
scrapy					
scrapy					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Scrapy is a high-level web crawling and scraping framework for Python. If you use \`HttpAuthMiddleware\` (i.e. the \`http_user\` and \`http_pass\` spider attributes) for HTTP authentication, all requests will expose your credentials to the request target. This includes requests generated by Scrapy components, such as \`robots.txt\` requests sent by Scrapy when the \`ROBOTSTXT_OBEY\` setting is set to \`True\`, or as requests reached through redirects. Upgrade to Scrapy 2.5.1 and use the new \`http_auth_domain\` spider attribute to control which domains are allowed to receive the configured HTTP authentication credentials. If you are using	https://github.com/scrapy/scrapy/commit/b01d69a1bf48060daec8f751368622352d8b85a6, https://github.com/scrapy/security/advisories/GHSA-jwqp-28gf-p498	A-SCR-SCRA-201021/311

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
			Scrapy 1.8 or a lower version, and upgrading to Scrapy 2.5.1 is not an option, you may upgrade to Scrapy 1.8.1 instead. If you cannot upgrade, set your HTTP authentication credentials on a per-request basis, using for example the `w3lib.http.basic_auth_header` function to convert your credentials into a value that you can assign to the `Authorization` header of your request, instead of defining your credentials globally using `HttpAuthMiddleware`. **CVE ID : CVE-2021-41125**		
Silverstripe					
silverstripe					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-21	4.3	SilverStripe Framework through 4.8.1 allows XSS. **CVE ID : CVE-2021-36150**	https://www.silverstripe.org/download/security-releases/CVE-2021-36150	A-SIL-SILV-201021/312
Incorrect Authorization	07-Oct-21	4	Default SilverStripe GraphQL Server (aka silverstripe/graphql) 3.x through 3.4.1 permission checker not inherited by query subclass. **CVE ID : CVE-2021-28661**	https://www.silverstripe.org/download/security-releases/CVE-2021-28661	A-SIL-SILV-201021/313
Sophos					

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
hitmanpro					
Improper Privilege Management	08-Oct-21	3.6	A local attacker could read or write arbitrary files with administrator privileges in HitmanPro before version Build 318. **CVE ID : CVE-2021-25271**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20211007-hmp-lpe	A-SOP-HITM-201021/314
hitmanpro.alert					
Improper Privilege Management	08-Oct-21	7.2	A local attacker could execute arbitrary code with administrator privileges in HitmanPro.Alert before version Build 901. **CVE ID : CVE-2021-25270**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20211007-hmpa-lpe	A-SOP-HITM-201021/315
spotweb_project					
spotweb					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in templates/installer/step-004.inc.php in spotweb 1.5.1 and below allow remote attackers to inject arbitrary web script or HTML via the newpassword2 parameter. **CVE ID : CVE-2021-40968**	N/A	A-SPO-SPOT-201021/316
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in templates/installer/step-004.inc.php in spotweb 1.5.1 and below allow remote attackers to inject arbitrary web script or HTML via the firstname parameter. **CVE ID : CVE-2021-40969**	N/A	A-SPO-SPOT-201021/317

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 Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in templates/installer/step-004.inc.php in spotweb 1.5.1 and below allow remote attackers to inject arbitrary web script or HTML via the username parameter. **CVE ID : CVE-2021-40970**	N/A	A-SPO-SPOT-201021/318
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in templates/installer/step-004.inc.php in spotweb 1.5.1 and below allow remote attackers to inject arbitrary web script or HTML via the newpassword1 parameter. **CVE ID : CVE-2021-40971**	N/A	A-SPO-SPOT-201021/319
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in templates/installer/step-004.inc.php in spotweb 1.5.1 and below allow remote attackers to inject arbitrary web script or HTML via the mail parameter. **CVE ID : CVE-2021-40972**	N/A	A-SPO-SPOT-201021/320
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	4.3	Cross-site scripting (XSS) vulnerability in templates/installer/step-004.inc.php in spotweb 1.5.1 and below allow remote attackers to inject arbitrary web script or HTML via the lastname parameter.	N/A	A-SPO-SPOT-201021/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40973		
sylius					
paypal					
Exposure of Sensitive Information to an Unauthorized Actor	05-Oct-21	5	sylius/paypal-plugin is a paypal plugin for the Sylius development platform. In affected versions the URL to the payment page done after checkout was created with autoincremented payment id (/pay-with-paypal/{id}) and therefore it was easy to predict. The problem is that the Credit card form has prefilled "credit card holder" field with the Customer's first and last name and hence this can lead to personally identifiable information exposure. Additionally, the mentioned form did not require authentication. The problem has been patched in Sylius/PayPalPlugin 1.2.4 and 1.3.1. If users are unable to update they can override a sylius_paypal_plugin_pay_with_paypal_form route and change its URL parameters to (for example) {orderToken}/{paymentId}, then override the Sylius\PayPalPlugin\Controller\PayWithPayPalFormAction service, to operate on the payment taken from the repository by these 2 values. It would also	https://github.com/Sylius/PayPalPlugin/commit/2adc46be2764ccee22b4247139b8056fb8d1afff, https://github.com/Sylius/PayPalPlugin/commit/814923c2e9d97fe6279dcee866c34ced3d2fb7a7, https://github.com/Sylius/PayPalPlugin/security/advisories/GHSA-25fx-mxc2-76g7	A-SYL-PAYP-201021/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			require usage of custom repository method. Additionally, one could override the @SyliusPayPalPlugin/payWithPaypal.html.twig template, to add contingencies: ['SCA_ALWAYS'] line in hostedFields.submit(...) function call (line 421). It would then have to be handled in the function callback. **CVE ID : CVE-2021-41120**		
tadtools_project					
tadtools					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Oct-21	4.3	TadTools special page parameter does not properly restrict the input of specific characters, thus remote attackers can inject JavaScript syntax without logging in, and further perform reflective XSS attacks. **CVE ID : CVE-2021-41565**	N/A	A-TAD-TADT-201021/323
Unrestricted Upload of File with Dangerous Type	08-Oct-21	7.5	The file extension of the TadTools file upload function fails to filter, thus remote attackers can upload any types of files and execute arbitrary code without logging in. **CVE ID : CVE-2021-41566**	N/A	A-TAD-TADT-201021/324
Incorrect Authorization	08-Oct-21	6.4	TadTools special page is vulnerable to authorization bypass, thus remote	N/A	A-TAD-TADT-201021/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers can use the specific parameter to delete arbitrary files in the system without logging in. **CVE ID : CVE-2021-41975**		
tad_book3_project					
tad_book3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Oct-21	4.3	Tad Book3 editing book function does not filter special characters. Unauthenticated attackers can remotely inject JavaScript syntax and execute stored XSS attacks. **CVE ID : CVE-2021-41563**	N/A	A-TAD-TAD_-201021/326
Incorrect Permission Assignment for Critical Resource	08-Oct-21	6.4	Tad Book3 editing book page does not perform identity verification. Remote attackers can use the vulnerability to view and modify arbitrary content of books without permission. **CVE ID : CVE-2021-41974**	N/A	A-TAD-TAD_-201021/327
tad_honor_project					
tad_honor					
Incorrect Authorization	08-Oct-21	5	Tad Honor viewing book list function is vulnerable to authorization bypass, thus remote attackers can use special parameters to delete articles arbitrarily without logging in. **CVE ID : CVE-2021-41564**	N/A	A-TAD-TAD_-201021/328
tad_uploader_project					
tad_uploader					

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 Input During Web Page Generation ('Cross-site Scripting')	08-Oct-21	4.3	The new add subject parameter of Tad Uploader view book list function fails to filter special characters. Unauthenticated attackers can remotely inject JavaScript syntax and execute stored XSS attacks. **CVE ID : CVE-2021-41567**	N/A	A-TAD-TAD_-201021/329
Incorrect Authorization	08-Oct-21	5	Tad Uploader edit book list function is vulnerable to authorization bypass, thus remote attackers can use the function to amend the folder names in the book list without logging in. **CVE ID : CVE-2021-41976**	N/A	A-TAD-TAD_-201021/330
tad_web_project					
tad_web					
Incorrect Authorization	08-Oct-21	6.4	Tad Web is vulnerable to authorization bypass, thus remote attackers can exploit the vulnerability to use the original function of viewing bulletin boards and uploading files in the system. **CVE ID : CVE-2021-41568**	N/A	A-TAD-TAD_-201021/331
teddy_project					
teddy					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-21	4.3	This affects the package teddy before 0.5.9. A type confusion vulnerability can be used to bypass input sanitization when the model content is an array (instead of a string).	https://github.com/rooseveltframework/teddy/pull/518	A-TED-TEDD-201021/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-23447		
Telegram					
telegram					
N/A	04-Oct-21	2.1	The Telegram application 7.5.0 through 7.8.0 for Android does not properly implement image self-destruction, a different vulnerability than CVE-2019-16248. After approximately two to four uses of the self-destruct feature, there is a misleading UI indication that an image was deleted (on both the sender and recipient sides). The images are still present in the /Storage/Emulated/0/Telegram/Telegram Image/ directory. **CVE ID : CVE-2021-41861**	https://telegram.org/blog/autodelete-inv2/ru#avtomaticheskoe-udalenie-soobschenii, https://desktop.telegram.org/changelog#v-2-6-23-02-21	A-TEL-TELE-201021/333
Thycotic					
secret_server					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Oct-21	4	A SQL injection issue was discovered in ThycoticCentrify Secret Server before 11.0.000007. The only affected versions are 10.9.000032 through 11.0.000006. **CVE ID : CVE-2021-41845**	https://docs.thycotic.com/bulletins/current/2021/11.0.000007.md, https://docs.thycotic.com/ss/11.0.0/release-notes/ss-rn-11-0-000007.md	A-THY-SECR-201021/334
Tibco					
activespaces					

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	05-Oct-21	6	The FTL Server (tibftlserver) and Docker images containing tibftlserver components of TIBCO Software Inc.'s TIBCO ActiveSpaces - Community Edition, TIBCO ActiveSpaces - Developer Edition, TIBCO ActiveSpaces - Enterprise Edition, TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, and TIBCO eFTL - Enterprise Edition contain a vulnerability that theoretically allows a non-administrative, authenticated FTL user to trick the affected components into creating illegitimate certificates. These maliciously generated certificates can be used to enable man-in-the-middle attacks or to escalate privileges so that the malicious user has administrative privileges. Affected releases are TIBCO Software Inc.'s TIBCO ActiveSpaces - Community Edition: versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.6.1, and 4.6.2, TIBCO ActiveSpaces - Developer Edition: versions 4.3.0, 4.4.0, 4.5.0, 4.6.0,	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2021/10/tibco-security-advisory-october-5-2021-tibco-ftl-2021-35497	A-TIB-ACTI-201021/335

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
			4.6.1, and 4.6.2, TIBCO ActiveSpaces - Enterprise Edition: versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.6.1, and 4.6.2, TIBCO FTL - Community Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO FTL - Developer Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO FTL - Enterprise Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO eFTL - Community Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO eFTL - Developer Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, and TIBCO eFTL - Enterprise Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0. **CVE ID : CVE-2021-35497**		
eftl					
Improper Certificate Validation	05-Oct-21	6	The FTL Server (tibftlserver) and Docker images containing tibftlserver components of TIBCO Software Inc.'s TIBCO ActiveSpaces - Community Edition, TIBCO ActiveSpaces - Developer Edition, TIBCO ActiveSpaces - Enterprise	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2021/10/tibco-security-advisory-	A-TIB-EFTL-201021/336

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
			Edition, TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, and TIBCO eFTL - Enterprise Edition contain a vulnerability that theoretically allows a non-administrative, authenticated FTL user to trick the affected components into creating illegitimate certificates. These maliciously generated certificates can be used to enable man-in-the-middle attacks or to escalate privileges so that the malicious user has administrative privileges. Affected releases are TIBCO Software Inc.'s TIBCO ActiveSpaces - Community Edition: versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.6.1, and 4.6.2, TIBCO ActiveSpaces - Developer Edition: versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.6.1, and 4.6.2, TIBCO ActiveSpaces - Enterprise Edition: versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.6.1, and 4.6.2, TIBCO FTL - Community Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO FTL - Developer Edition: versions	october-5-2021-tibco-ftl-2021-35497	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO FTL - Enterprise Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO eFTL - Community Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO eFTL - Developer Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, and TIBCO eFTL - Enterprise Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0. **CVE ID : CVE-2021-35497**		
ftl					
Improper Certificate Validation	05-Oct-21	6	The FTL Server (tibftlserver) and Docker images containing tibftlserver components of TIBCO Software Inc.'s TIBCO ActiveSpaces - Community Edition, TIBCO ActiveSpaces - Developer Edition, TIBCO ActiveSpaces - Enterprise Edition, TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, and TIBCO eFTL - Enterprise Edition contain a vulnerability that	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2021/10/tibco-security-advisory-october-5-2021-tibco-ftl-2021-35497	A-TIB-FTL-201021/337

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
		🟧	theoretically allows a non-administrative, authenticated FTL user to trick the affected components into creating illegitimate certificates. These maliciously generated certificates can be used to enable man-in-the-middle attacks or to escalate privileges so that the malicious user has administrative privileges. Affected releases are TIBCO Software Inc.'s TIBCO ActiveSpaces - Community Edition: versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.6.1, and 4.6.2, TIBCO ActiveSpaces - Developer Edition: versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.6.1, and 4.6.2, TIBCO ActiveSpaces - Enterprise Edition: versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.6.1, and 4.6.2, TIBCO FTL - Community Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO FTL - Developer Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO FTL - Enterprise Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, TIBCO eFTL - Community Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0,		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TIBCO eFTL - Developer Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0, and TIBCO eFTL - Enterprise Edition: versions 6.2.0, 6.3.0, 6.3.1, 6.4.0, 6.5.0, 6.6.0, 6.6.1, and 6.7.0. **CVE ID : CVE-2021-35497**		
Tipsandtricks-hq					
software_license_manager					
Cross-Site Request Forgery (CSRF)	11-Oct-21	6.8	The del_reistered_domains AJAX action of the Software License Manager WordPress plugin before 4.5.1 does not have any CSRF checks, and is vulnerable to a CSRF attack **CVE ID : CVE-2021-24711**	N/A	A-TIP-SOFT-201021/338
Trendmicro					
apex_one					
Improper Privilege Management	06-Oct-21	2.1	An arbitrary file creation by privilege escalation vulnerability in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1, and Worry-Free Business Security Services could allow a local attacker to create an arbitrary file with higher privileges that could lead to a denial-of-service (DoS) on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the	https://success.trendmicro.com/solution/000289183	A-TRE-APEX-201021/339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			target system in order to exploit this vulnerability. **CVE ID : CVE-2021-3848**		
worry-free_business_security					
Improper Privilege Management	06-Oct-21	2.1	An arbitrary file creation by privilege escalation vulnerability in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1, and Worry-Free Business Security Services could allow a local attacker to create an arbitrary file with higher privileges that could lead to a denial-of-service (DoS) on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-3848**	https://success.trendmicro.com/solution/000289183	A-TRE-WORR-201021/340
Typo3					
typo3					
Cross-Site Request Forgery (CSRF)	05-Oct-21	6.8	TYPO3 is an open source PHP based web content management system released under the GNU GPL. It has been discovered that the new TYPO3 v11 feature that allows users to create and share deep links in the backend user interface is vulnerable to cross-site-request-forgery. The impact is the same as described in TYPO3-CORE-	https://github.com/TYPO3/typo3/commit/fa51999203c5e5d913ecae5ea843ccb2b95fa33f, https://github.com/TYPO3/typo3/security/advisories/GHSA-657m-v5vm-f6rw,	A-TYP-TYPO-201021/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA-2020-006 (CVE-2020-11069). However, it is not limited to the same site context and does not require the attacker to be authenticated. In a worst case scenario, the attacker could create a new admin user account to compromise the system. To successfully carry out an attack, an attacker must trick his victim to access a compromised system. The victim must have an active session in the TYPO3 backend at that time. The following Same-Site cookie settings in $GLOBALS[TYPO3_CONF_VARS][BE][cookieSameSite] are required for an attack to be successful: SameSite=strict: malicious evil.example.org invoking TYPO3 application at good.example.org and SameSite=lax or none: malicious evil.com invoking TYPO3 application at example.org. Update your instance to TYPO3 version 11.5.0 which addresses the problem described. **CVE ID : CVE-2021-41113**	https://typo3.org/security/advisory/typo3-core-sa-2020-006	
Improper Input Validation	05-Oct-21	5	TYPO3 is an open source PHP based web content management system released under the GNU GPL. It has been discovered	https://github.com/TYPO3/typo3/security/advisories/GHSA-m2jh-	A-TYP-TYPO-201021/342

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
			that TYPO3 CMS is susceptible to host spoofing due to improper validation of the HTTP Host header. TYPO3 uses the HTTP Host header, for example, to generate absolute URLs during the frontend rendering process. Since the host header itself is provided by the client, it can be forged to any value, even in a name-based virtual hosts environment. This vulnerability is the same as described in TYPO3-CORE-SA-2014-001 (CVE-2014-3941). A regression, introduced during TYPO3 v11 development, led to this situation. The already existing setting $GLOBALS['TYPO3_CONF_VARS']['SYS']['trustedHostsPattern'] (used as an effective mitigation strategy in previous TYPO3 versions) was not evaluated anymore, and reintroduced the vulnerability. **CVE ID : CVE-2021-41114**	fxw4-gphm, https://github.com/TYPO3/typo3/commit/5cbff85506cebe343e5ae59228977547cf8e3cf4, https://typo3.org/security/advisory/typo3-core-sa-2021-015	
verint					
workforce_optimization					
Improper Neutralization of Special Elements in Output Used	08-Oct-21	5	Verint Workforce Optimization (WFO) 15.2.5.1033 allows HTML injection via the /wfo/control/signin	https://www.verint.com/engagement/our-offerings/solu	A-VER-WORK-201021/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
by a Downstream Component ('Injection')			username parameter. **CVE ID : CVE-2021-41825**	tions/workforce-optimization/	
vyper_project					
vyper					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Oct-21	6.5	Vyper is a Pythonic Smart Contract Language for the EVM. In affected versions when performing a function call inside a literal struct, there is a memory corruption issue that occurs because of an incorrect pointer to the the top of the stack. This issue has been resolved in version 0.3.0. **CVE ID : CVE-2021-41121**	https://github.com/vyperlang/vyper/security/advisories/GHSA-xv8x-pr4h-73jv, https://github.com/vyperlang/vyper/pull/2447	A-VYP-VYPE-201021/344
Incorrect Calculation	05-Oct-21	4	Vyper is a Pythonic Smart Contract Language for the EVM. In affected versions external functions did not properly validate the bounds of decimal arguments. The can lead to logic errors. This issue has been resolved in version 0.3.0. **CVE ID : CVE-2021-41122**	https://github.com/vyperlang/vyper/security/advisories/GHSA-c7pr-343r-5c46	A-VYP-VYPE-201021/345
webnus					
modern_events_calendar_lite					
Improper Neutralization of Input During Web Page Generation	04-Oct-21	3.5	The Modern Events Calendar Lite WordPress plugin before 5.22.2 does not escape some of its settings before outputting them in attributes, allowing	N/A	A-WEB-MODE-201021/346

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
('Cross-site Scripting')			high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24687**		
webtareas_project					
webtareas					
Cross-Site Request Forgery (CSRF)	08-Oct-21	6.8	A Cross-Site Request Forgery (CSRF) vulnerability in webTareas version 2.4 and earlier allows a remote attacker to create a new administrative profile and add a new user to the new profile. without the victim's knowledge, by enticing an authenticated admin user to visit an attacker's web page. **CVE ID : CVE-2021-41916**	N/A	A-WEB-WEBT-201021/347
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Oct-21	3.5	webTareas version 2.4 and earlier allows an authenticated user to store arbitrary web script or HTML by creating or editing a client name in the clients section, due to incorrect sanitization of user-supplied data and achieve a Stored Cross-Site Scripting attack against the platform users and administrators. The affected endpoint is /clients/editclient.php, on the HTTP POST cn parameter.	N/A	A-WEB-WEBT-201021/348

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
			CVE ID : CVE-2021-41917		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Oct-21	3.5	webTareas version 2.4 and earlier allows an authenticated user to inject arbitrary web script or HTML due to incorrect sanitization of user-supplied data and achieve a Reflected Cross-Site Scripting attack against the platform users and administrators. The issue affects every endpoint on the application because it is related on how each URL is echoed back on every response page. **CVE ID : CVE-2021-41918**	N/A	A-WEB-WEBT-201021/349
Unrestricted Upload of File with Dangerous Type	08-Oct-21	6.5	webTareas version 2.4 and earlier allows an authenticated user to arbitrarily upload potentially dangerous files without restrictions. This is working by adding or replacing a personal profile picture. The affected endpoint is /includes/upload.php on the HTTP POST data. This allows an attacker to exploit the platform by injecting code or malware and, under certain conditions, to execute code on remote user browsers. **CVE ID : CVE-2021-41919**	N/A	A-WEB-WEBT-201021/350
Improper Neutralizatio	08-Oct-21	5	webTareas version 2.4 and earlier allows an	N/A	A-WEB-WEBT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an SQL Command ('SQL Injection')			unauthenticated user to perform Time and Boolean-based blind SQL Injection on the endpoint /includes/library.php, via the sor_cible, sor_champs, and sor_ordre HTTP POST parameters. This allows an attacker to access all the data in the database and obtain access to the webTareas application. **CVE ID : CVE-2021-41920**		201021/351
wire					
wire					
Improper Authorization	04-Oct-21	7.5	Wire is an open source secure messenger. In affected versions if the an attacker gets an old but valid access token they can take over an account by changing the email. This issue has been resolved in version 3.86 which uses a new endpoint which additionally requires an authentication cookie. See wire-ios-sync-engine and wire-ios-transport references. This is the root advisory that pulls the changes together. **CVE ID : CVE-2021-41093**	https://github.com/wireapp/wire-ios/commit/b0e7bb3b13dd8212032cb46e32edf701694687c7, https://github.com/wireapp/wire-ios/security/advisories/GHSA-6f4c-phfj-m255	A-WIR-WIRE-201021/352
Exposure of Resource to Wrong Sphere	04-Oct-21	2.1	Wire is an open source secure messenger. Users of Wire by Bund may bypass the mandatory encryption at rest feature by simply disabling their device	https://github.com/wireapp/wire-ios/commit/5ba3eb180efc3fc795d095f9c	A-WIR-WIRE-201021/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passcode. Upon launching, the app will attempt to enable encryption at rest by generating encryption keys via the Secure Enclave, however it will fail silently if no device passcode is set. The user has no indication that encryption at rest is not active since the feature is hidden to them. This issue has been resolved in version 3.70 **CVE ID : CVE-2021-41094**	84ae7f109b84746, https://github.com/wireapp/wire-ios/security/advisories/GHSA-h4m7-pr8h-j7rf	
wire-server					
Insufficient Session Expiration	04-Oct-21	7.5	Wire-server is the backing server for the open source wire secure messaging application. In affected versions it is possible to trigger email address change of a user with only the short-lived session token in the `Authorization` header. As the short-lived token is only meant as means of authentication by the client for less critical requests to the backend, the ability to change the email address with a short-lived token constitutes a privilege escalation attack. Since the attacker can change the password after setting the email address to one that they control, changing the email address can result in an account	https://github.com/wireapp/wire-server/security/advisories/GHSA-9rm2-w6pq-333m	A-WIR-WIRE-201021/354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			takeover by the attacker. Short-lived tokens can be requested from the backend by Wire clients using the long lived tokens, after which the long lived tokens can be stored securely, for example on the devices key chain. The short lived tokens can then be used to authenticate the client towards the backend for frequently performed actions such as sending and receiving messages. While short-lived tokens should not be available to an attacker per-se, they are used more often and in the shape of an HTTP header, increasing the risk of exposure to an attacker relative to the long-lived tokens, which are stored and transmitted in cookies. If you are running an on-prem instance and provision all users with SCIM, you are not affected by this issue (changing email is blocked for SCIM users). SAML single-sign-on is unaffected by this issue, and behaves identically before and after this update. The reason is that the email address used as SAML NameID is stored in a different location in the databse from the one used to contact the user outside		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			wire. Version 2021-08-16 and later provide a new end-point that requires both the long-lived client cookie and `Authorization` header. The old end-point has been removed. If you are running an on-prem instance with at least some of the users invited or provisioned via SAML SSO and you cannot update then you can block `/self/email` on nginz (or in any other proxies or firewalls you may have set up). You don't need to discriminate by verb: `/self/email` only accepts `PUT` and `DELETE`, and `DELETE` is almost never used. **CVE ID : CVE-2021-41100**		
wowza					
streaming_engine					
Cross-Site Request Forgery (CSRF)	05-Oct-21	5.8	A Cross-Site Request Forgery (CSRF) vulnerability in Wowza Streaming Engine through 4.8.11+5 allows a remote attacker to delete a user account via the /enginemanager/server/user/delete.htm userName parameter. The application does not implement a CSRF token for the GET request. **CVE ID : CVE-2021-35491**	https://www.wowza.com/docs/wowza-streaming-engine-4-8-14-release-notes	A-WOW-STRE-201021/355
Uncontrolled	05-Oct-21	4	Wowza Streaming Engine	https://www.	A-WOW-

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
Resource Consumption			through 4.8.11+5 could allow an authenticated, remote attacker to exhaust filesystem resources via the /enginemanager/server/vhost/historical.jsdata vhost parameter. This is due to the insufficient management of available filesystem resources. An attacker could exploit this vulnerability through the Virtual Host Monitoring section by requesting random virtual-host historical data and exhausting available filesystem resources. A successful exploit could allow the attacker to cause database errors and cause the device to become unresponsive to web-based management. (Manual intervention is required to free filesystem resources and return the application to an operational state.) **CVE ID : CVE-2021-35492**	wowza.com/docs/wowza-streaming-engine-4-8-14-release-notes	STRE-201021/356
wpbrigade					
simple_social_buttons					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-21	3.5	The Simple Social Media Share Buttons WordPress plugin before 3.2.4 does not escape the Share Title settings before outputting it in the frontend pages or posts (depending on the settings used), allowing high privilege users to	N/A	A-WPB-SIMP-201021/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24656**		
wpdevart					
coming_soon_and_maintenance_mode					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-21	3.5	The Coming soon and Maintenance mode WordPress plugin before 3.5.3 does not properly sanitize inputs submitted by authenticated users when setting adding or modifying coming soon or maintenance mode pages, leading to stored XSS. **CVE ID : CVE-2021-24577**	N/A	A-WPD-COMI-201021/358
wpeverest					
user_registration					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-21	3.5	The User Registration WordPress plugin before 2.0.2 does not properly sanitise the user_registration_profile_pic_url value when submitted directly via the user_registration_update_profile_details AJAX action. This could allow any authenticated user, such as subscriber, to perform Stored Cross-Site attacks when their profile is viewed **CVE ID : CVE-2021-24654**	N/A	A-WPE-USER-201021/359
wp_bannerize_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wp_bannerize					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-21	4	The WP Bannerize WordPress plugin is vulnerable to authenticated SQL injection via the id parameter found in the ~/Classes/wpBannerizeAdmin.php file which allows attackers to exfiltrate sensitive information from vulnerable sites. This issue affects versions 2.0.0 - 4.0.2. **CVE ID : CVE-2021-39351**	https://plugins.trac.wordpress.org/browser/wp-bannerize/trunk/Classes/wpBannerizeAdmin.php#L1681	A-WP_-WP_B-201021/360
wp_html_author_bio_project					
wp_html_author_bio					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-21	3.5	The WP HTML Author Bio WordPress plugin through 1.2.0 does not sanitise the HTML allowed in the Bio of users, allowing them to use malicious JavaScript code, which will be executed when anyone visit a post in the frontend made by such user. As a result, user with a role as low as author could perform Cross-Site Scripting attacks against users, which could potentially lead to privilege escalation when an admin view the related post/s. **CVE ID : CVE-2021-24545**	N/A	A-WP_-WP_H-201021/361
Zammad					
Zammad					
Loop with Unreachable	07-Oct-21	4	An issue was discovered in Zammad before 4.1.1. An	https://zammad.com/en/ad	A-ZAM-ZAMM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exit Condition ('Infinite Loop')			attacker with valid agent credentials may send a series of crafted requests that cause an endless loop and thus cause denial of service. **CVE ID : CVE-2021-42084**	visories/zaa-2021-11	201021/362
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-21	3.5	An issue was discovered in Zammad before 4.1.1. There is stored XSS via a custom Avatar. **CVE ID : CVE-2021-42085**	https://zammad.com/en/advisories/zaa-2021-17	A-ZAM-ZAMM-201021/363
Improper Privilege Management	07-Oct-21	6.5	An issue was discovered in Zammad before 4.1.1. An Agent account can modify account data, and gain admin access, via a crafted request. **CVE ID : CVE-2021-42086**	https://zammad.com/en/advisories/zaa-2021-09	A-ZAM-ZAMM-201021/364
Exposure of Resource to Wrong Sphere	07-Oct-21	4	An issue was discovered in Zammad before 4.1.1. An admin can discover the application secret via the API. **CVE ID : CVE-2021-42087**	https://zammad.com/en/advisories/zaa-2021-15	A-ZAM-ZAMM-201021/365
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-21	4.3	An issue was discovered in Zammad before 4.1.1. The Chat functionality allows XSS because clipboard data is mishandled. **CVE ID : CVE-2021-42088**	https://zammad.com/en/advisories/zaa-2021-12	A-ZAM-ZAMM-201021/366
Exposure of Sensitive	07-Oct-21	5	An issue was discovered in Zammad before 4.1.1. The	https://zammad.com/en/ad	A-ZAM-ZAMM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information to an Unauthorized Actor			REST API discloses sensitive information. **CVE ID : CVE-2021-42089**	visories/zaa-2021-13	201021/367
Deserialization of Untrusted Data	07-Oct-21	7.5	An issue was discovered in Zammad before 4.1.1. The Form functionality allows remote code execution because deserialization is mishandled. **CVE ID : CVE-2021-42090**	https://zammad.com/en/advisories/zaa-2021-14	A-ZAM-ZAMM-201021/368
Server-Side Request Forgery (SSRF)	07-Oct-21	6.4	An issue was discovered in Zammad before 4.1.1. SSRF can occur via GitHub or GitLab integration. **CVE ID : CVE-2021-42091**	https://zammad.com/en/advisories/zaa-2021-08	A-ZAM-ZAMM-201021/369
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-21	3.5	An issue was discovered in Zammad before 4.1.1. Stored XSS may occur via an Article during addition of an attachment to a Ticket. **CVE ID : CVE-2021-42092**	https://zammad.com/en/advisories/zaa-2021-16	A-ZAM-ZAMM-201021/370
N/A	07-Oct-21	6.5	An issue was discovered in Zammad before 4.1.1. An admin can execute code on the server via a crafted request that manipulates triggers. **CVE ID : CVE-2021-42093**	https://zammad.com/en/advisories/zaa-2021-10	A-ZAM-ZAMM-201021/371
Improper Neutralization of Special Elements used in a Command ('Command	07-Oct-21	7.5	An issue was discovered in Zammad before 4.1.1. Command Injection can occur via custom Packages. **CVE ID : CVE-2021-42094**	https://zammad.com/en/advisories/zaa-2021-18	A-ZAM-ZAMM-201021/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')					
Zohocorp					
manageengine_admanager_plus					
Unrestricted Upload of File with Dangerous Type	07-Oct-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file overwrite leading to remote code execution. **CVE ID : CVE-2021-37762**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-201021/373
Unrestricted Upload of File with Dangerous Type	07-Oct-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution. **CVE ID : CVE-2021-37918**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-201021/374
Unrestricted Upload of File with Dangerous Type	07-Oct-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution. **CVE ID : CVE-2021-37919**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-201021/375
Unrestricted Upload of File with Dangerous Type	07-Oct-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution. **CVE ID : CVE-2021-37920**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-201021/376
Unrestricted Upload of File with Dangerous	07-Oct-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload	https://www.manageengine.com/products/ad-	A-ZOH-MANA-201021/377

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
Type			which leads to remote code execution. **CVE ID : CVE-2021-37921**	manager/release-notes.html#7111	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Oct-21	5	Zoho ManageEngine ADManager Plus version 7110 and prior is vulnerable to path traversal which allows copying of files from one directory to another. **CVE ID : CVE-2021-37922**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-201021/378
Unrestricted Upload of File with Dangerous Type	07-Oct-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution. **CVE ID : CVE-2021-37923**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-201021/379
Unrestricted Upload of File with Dangerous Type	07-Oct-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution. **CVE ID : CVE-2021-37924**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-201021/380
Unrestricted Upload of File with Dangerous Type	07-Oct-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution. **CVE ID : CVE-2021-37926**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-201021/381
Unrestricted Upload of File with	07-Oct-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows	https://www.manageengine.com/produc	A-ZOH-MANA-201021/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			unrestricted file upload which leads to remote code execution. **CVE ID : CVE-2021-37928**	ts/ad-manager/release-notes.html#7111	
Unrestricted Upload of File with Dangerous Type	07-Oct-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution. **CVE ID : CVE-2021-37929**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-201021/383
Unrestricted Upload of File with Dangerous Type	07-Oct-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution. **CVE ID : CVE-2021-37930**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-201021/384
Unrestricted Upload of File with Dangerous Type	07-Oct-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows unrestricted file upload which leads to remote code execution. **CVE ID : CVE-2021-37931**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-201021/385
Improper Restriction of XML External Entity Reference	07-Oct-21	7.5	Zoho ManageEngine ADManager Plus before 7110 is vulnerable to blind XXE. **CVE ID : CVE-2021-38298**	https://www.manageengine.com/products/ad-manager/release-notes.html#7110	A-ZOH-MANA-201021/386
zoho_crm_lead_magnet					
Improper	05-Oct-21	3.5	A Cross-Site Scripting (XSS)	N/A	A-ZOH-ZOHO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			attack can cause arbitrary code (JavaScript) to run in a user's browser while the browser is connected to a trusted website. The attack targets your application's users and not the application itself while using your application as the attack's vehicle. The XSS payload executes whenever the user changes the form values or deletes a created form in Zoho CRM Lead Magnet Version 1.7.2.4. **CVE ID : CVE-2021-33849**		201021/387
Zulip					
Zulip					
N/A	07-Oct-21	4	Zulip is an open source team chat server. In affected versions Zulip allows organization administrators on a server to configure "linkifiers" that automatically create links from messages that users send, detected via arbitrary regular expressions. Malicious organization administrators could subject the server to a denial-of-service via regular expression complexity attacks; most simply, by configuring a quadratic-time regular expression in a linkifier, and sending messages that	https://github.com/zulip/zulip/security/advisories/GHSA-4h36-mqfq-42jg, https://github.com/zulip/zulip/commit/e2d303c1bb5f538d17dc3d9134bc8858bdece781	A-ZUL-ZULI-201021/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploited it. A regular expression attempted to parse the user-provided regexes to verify that they were safe from ReDoS -- this was both insufficient, as well as _itself_ subject to ReDoS if the organization administrator entered a sufficiently complex invalid regex. Affected users should [upgrade to the just-released Zulip 4.7](https://zulip.readthedocs.io/en/latest/production/upgrade-or-modify.html#upgrading-to-a-release), or [`main`](https://zulip.readthedocs.io/en/latest/production/upgrade-or-modify.html#upgrading-from-a-git-repository). **CVE ID : CVE-2021-41115**		
zyte					
scrapy-splash					
Exposure of Sensitive Information to an Unauthorized Actor	05-Oct-21	4.3	Scrapy-splash is a library which provides Scrapy and JavaScript integration. In affected versions users who use [`HttpAuthMiddleware`](http://doc.scrapy.org/en/latest/topics/downloader-middleware.html#module-scrapy.downloadermiddlewares.httpauth) (i.e. the `http_user` and `http_pass` spider attributes) for Splash authentication will	https://github.com/scrapy-plugins/scrapy-splash/commit/2b253e57fe64ec575079c8cdc99fe2013502ea31, https://github.com/scrapy-plugins/scrap	A-ZYT-SCRA-201021/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have any non-Splash request expose your credentials to the request target. This includes `robots.txt` requests sent by Scrapy when the `ROBOTSTXT_OBEY` setting is set to `True`. Upgrade to scrapy-splash 0.8.0 and use the new `SPLASH_USER` and `SPLASH_PASS` settings instead to set your Splash authentication credentials safely. If you cannot upgrade, set your Splash request credentials on a per-request basis, [using the `splash_headers` request parameter](https://github.com/scrapy-plugins/scrapy-splash/tree/0.8.x#http-basic-auth), instead of defining them globally using the [`HttpAuthMiddleware`](http://doc.scrapy.org/en/latest/topics/downloader-middleware.html#module-scrapy.downloadermiddlewares.httpauth). Alternatively, make sure all your requests go through Splash. That includes disabling the [robots.txt middleware](https://docs.scrapy.org/en/latest/topics/downloader-middleware.html#topics-	y-splash/security/advisories/GHSA-823f-cwm9-4g74	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			dlmw-robots). **CVE ID : CVE-2021-41124**		
Hardware					
bosch					
indracontrol_xlc					
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-INDR-201021/390
rexroth_indramotion_mlc					
Use of Password Hash With Insufficient Computational Effort	04-Oct-21	5	The user and password data base is exposed by an unprotected web server resource. Passwords are hashed with a weak hashing algorithm and therefore allow an attacker to determine the password by using rainbow tables. **CVE ID : CVE-2021-23855**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/391
rexroth_indramotion_mlc_l20					
Improper Neutralization of Input During Web Page	04-Oct-21	4.3	The web server is vulnerable to reflected XSS and therefore an attacker might be able to execute scripts on a client's	https://psirt.bosch.com/security-advisories/bosch-sa-	H-BOS-REXR-201021/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			computer by sending the client a manipulated URL. **CVE ID : CVE-2021-23856**	741752.html	
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/393
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/394
rexroth_indramotion_mlc_l25					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/395

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
			system. **CVE ID : CVE-2021-23857**		
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/396
rexroth_indramotion_mlc_l40					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-21	4.3	The web server is vulnerable to reflected XSS and therefore an attacker might be able to execute scripts on a client's computer by sending the client a manipulated URL. **CVE ID : CVE-2021-23856**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/397
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/398
Insufficiently	04-Oct-21	7.8	Information disclosure:	https://psirt.	H-BOS-REXR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	bosch.com/security-advisories/bosch-sa-741752.html	201021/399
rexroth_indramotion_mlc_l45					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/400
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/401

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
			server resource. **CVE ID : CVE-2021-23858**		
rexroth_indramotion_mlc_l65					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/402
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/403
rexroth_indramotion_mlc_l75					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subsequently login to the system. **CVE ID : CVE-2021-23857**		
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/405
rexroth_indramotion_mlc_l85					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/406
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**		
rexroth_indramotion_mlc_xm21					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/408
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/409
rexroth_indramotion_mlc_xm22					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by	https://psirt.bosch.com/security-advisories/bo	H-BOS-REXR-201021/410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	sch-sa-741752.html	
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/411
rexroth_indramotion_mlc_xm41					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/412
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected	https://psirt.bosch.com/security-advisories/bosch-sa-	H-BOS-REXR-201021/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	741752.html	
rexroth_indramotion_mlc_xm42					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/414
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/415
rexroth_indramotion_xlc					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Password Hash With Insufficient Computational Effort	04-Oct-21	5	The user and password data base is exposed by an unprotected web server resource. Passwords are hashed with a weak hashing algorithm and therefore allow an attacker to determine the password by using rainbow tables. **CVE ID : CVE-2021-23855**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/416
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	H-BOS-REXR-201021/417
bostonscientific					
zoom_latitude_pogrammer\\/recorder\\/monitor_3120					
Improper Access Control	04-Oct-21	7.2	A skilled attacker with physical access to the affected device can gain access to the hard disk drive of the device to change the telemetry region and could use this setting to interrogate or program an implantable device in any region in the world. **CVE ID : CVE-2021-38392**	N/A	H-BOS-ZOOM-201021/418
Missing Protection Against	04-Oct-21	6.9	An attacker with physical access to the device can extract the binary that	N/A	H-BOS-ZOOM-201021/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques			checks for the hardware key and reverse engineer it, which could be used to create a physical duplicate of a valid hardware key. The hardware key allows access to special settings when inserted. **CVE ID : CVE-2021-38394**		
Insufficient Verification of Data Authenticity	04-Oct-21	4.6	The programmer installation utility does not perform a cryptographic authenticity or integrity checks of the software on the flash drive. An attacker could leverage this weakness to install unauthorized software using a specially crafted USB. **CVE ID : CVE-2021-38396**	N/A	H-BOS-ZOOM-201021/420
N/A	04-Oct-21	4.6	The affected device uses off-the-shelf software components that contain unpatched vulnerabilities. A malicious attacker with physical access to the affected device could exploit these vulnerabilities. **CVE ID : CVE-2021-38398**	N/A	H-BOS-ZOOM-201021/421
Use of Password Hash With Insufficient Computation al Effort	04-Oct-21	4.6	An attacker with physical access to Boston Scientific Zoom Latitude Model 3120 can remove the hard disk drive or create a specially crafted USB to extract the password hash for brute force reverse engineering	N/A	H-BOS-ZOOM-201021/422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the system password. **CVE ID : CVE-2021-38400**		
zoom_latitude_programming_system_model_3120					
N/A	04-Oct-21	4.6	The affected device uses off-the-shelf software components that contain unpatched vulnerabilities. A malicious attacker with physical access to the affected device could exploit these vulnerabilities. **CVE ID : CVE-2021-38398**	N/A	H-BOS-ZOOM-201021/423
Cisco					
ata_190					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	9	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34710**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-A4J57F3	H-CIS-ATA_-201021/424
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	7.8	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-	H-CIS-ATA_-201021/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34735**	A4J57F3	
ata_191					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	9	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34710**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-A4J57F3	H-CIS-ATA_-201021/426
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	7.8	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34735**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-A4J57F3	H-CIS-ATA_-201021/427
ata_192					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	9	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34710**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-A4J57F3	H-CIS-ATA_-201021/428
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	7.8	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34735**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-A4J57F3	H-CIS-ATA_-201021/429
business_220-16p-2g					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/431
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/432

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/433
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/437
business_220-16t-2g					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/438

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
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/439
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/440

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/441
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/445
business_220-24fp-4g					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/446

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
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/447
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/448

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/449
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/453
business_220-24fp-4x					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/455
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/457
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/461
business_220-24p-4g					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/462

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
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/463
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/464

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/465
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/469
business_220-24p-4x					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/470

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
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/471
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/472

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/473
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/474

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
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/476

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
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/477
business_220-24t-4g					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/479
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/480

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/481
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/483

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 about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/484

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
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/485
business_220-24t-4x					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/487
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/489
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/490

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
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/493
business_220-48fp-4x					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/495
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/496

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/497
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/500

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
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/501
business_220-48p-4g					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/503
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/504

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/505
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/509
business_220-48p-4x					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/511
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/513
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/514

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
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/515

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 about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/517
business_220-48t-4g					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/518

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
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/519
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/521
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/525
business_220-48t-4x					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/526

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
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/527
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/528

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/529
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/533
business_220-8fp-e-2g					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/535
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/536

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/537
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/541
business_220-8p-e-2g					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/542

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
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/543
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/544

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/545
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/546

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
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/549
business_220-8t-e-2g					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-	H-CIS-BUSI-201021/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	cred-MJCEXvX	
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	H-CIS-BUSI-201021/551
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/552

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/553
Buffer Copy without	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer	https://tools.cisco.com/sec	H-CIS-BUSI-201021/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	H-CIS-BUSI-201021/557
email_security_appliance_c170					
N/A	06-Oct-21	5	A vulnerability in the antispam protection mechanisms of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-	H-CIS-EMAI-201021/558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2021-1534**	sGcfsDrp	
email_security_appliance_c190					
N/A	06-Oct-21	5	A vulnerability in the antispam protection mechanisms of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-sGcfsDrp	H-CIS-EMAI-201021/559

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-2021-1534		
email_security_appliance_c380					
N/A	06-Oct-21	5	A vulnerability in the antispam protection mechanisms of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2021-1534**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-sGcfsDrp	H-CIS-EMAI-201021/560
email_security_appliance_c390					
N/A	06-Oct-21	5	A vulnerability in the antispam protection mechanisms of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-sGcfsDrp	H-CIS-EMAI-201021/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2021-1534**		
email_security_appliance_c680					
N/A	06-Oct-21	5	A vulnerability in the antispam protection mechanisms of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2021-1534**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-sGcfsDrp	H-CIS-EMAI-201021/562
email_security_appliance_c690					
N/A	06-Oct-21	5	A vulnerability in the	https://tools.	H-CIS-EMAI-

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
			antispam protection mechanisms of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2021-1534**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-sGcfsDrp	201021/563
email_security_appliance_c690x					
N/A	06-Oct-21	5	A vulnerability in the antispam protection mechanisms of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-sGcfsDrp	H-CIS-EMAI-201021/564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2021-1534**		
ip_conference_phone_7832					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_C-201021/565
ip_conference_phone_8832					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_C-201021/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**		
ip_phones_8832					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_P-201021/567
ip_phone_7811					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_P-201021/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**		
ip_phone_7821					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_P-201021/569
ip_phone_7832					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_P-201021/570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**		
ip_phone_7841					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_P-201021/571
ip_phone_7861					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_P-201021/572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**		
ip_phone_8811					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_P-201021/573
ip_phone_8831					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_P-201021/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			any file on the device file system. **CVE ID : CVE-2021-34711**		
ip_phone_8841					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_P-201021/575
ip_phone_8845					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_P-201021/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system. **CVE ID : CVE-2021-34711**		
ip_phone_8851					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_P-201021/577
ip_phone_8861					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_P-201021/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34711		
ip_phone_8865					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-IP_P-201021/579
web_security_appliance_s170					
Missing Release of Memory after Effective Lifetime	06-Oct-21	7.8	A vulnerability in the proxy service of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to exhaust system memory and cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper memory management in the proxy service of an affected device. An attacker could exploit this vulnerability by establishing a large number of HTTPS connections to the affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-dos-fmHdKswk	H-CIS-WEB_-201021/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the system to stop processing new connections, which could result in a DoS condition. Note: Manual intervention may be required to recover from this situation. **CVE ID : CVE-2021-34698**		
web_security_appliance_s190					
Missing Release of Memory after Effective Lifetime	06-Oct-21	7.8	A vulnerability in the proxy service of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to exhaust system memory and cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper memory management in the proxy service of an affected device. An attacker could exploit this vulnerability by establishing a large number of HTTPS connections to the affected device. A successful exploit could allow the attacker to cause the system to stop processing new connections, which could result in a DoS condition. Note: Manual intervention may be required to recover from this situation. **CVE ID : CVE-2021-34698**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-dos-fmHdKswk	H-CIS-WEB_-201021/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
web_security_appliance_s380					
Missing Release of Memory after Effective Lifetime	06-Oct-21	7.8	A vulnerability in the proxy service of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to exhaust system memory and cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper memory management in the proxy service of an affected device. An attacker could exploit this vulnerability by establishing a large number of HTTPS connections to the affected device. A successful exploit could allow the attacker to cause the system to stop processing new connections, which could result in a DoS condition. Note: Manual intervention may be required to recover from this situation. **CVE ID : CVE-2021-34698**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-dos-fmHdKswk	H-CIS-WEB_-201021/582
web_security_appliance_s390					
Missing Release of Memory after Effective Lifetime	06-Oct-21	7.8	A vulnerability in the proxy service of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to exhaust system memory and cause a denial of service (DoS) condition on an affected device. This vulnerability is	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-dos-fmHdKswk	H-CIS-WEB_-201021/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to improper memory management in the proxy service of an affected device. An attacker could exploit this vulnerability by establishing a large number of HTTPS connections to the affected device. A successful exploit could allow the attacker to cause the system to stop processing new connections, which could result in a DoS condition. Note: Manual intervention may be required to recover from this situation. **CVE ID : CVE-2021-34698**		
web_security_appliance_s680					
Missing Release of Memory after Effective Lifetime	06-Oct-21	7.8	A vulnerability in the proxy service of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to exhaust system memory and cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper memory management in the proxy service of an affected device. An attacker could exploit this vulnerability by establishing a large number of HTTPS connections to the affected device. A successful exploit could allow the attacker to cause the system to stop	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-dos-fmHdKswk	H-CIS-WEB_-201021/584

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
			processing new connections, which could result in a DoS condition. Note: Manual intervention may be required to recover from this situation. **CVE ID : CVE-2021-34698**		
web_security_appliance_s690					
Missing Release of Memory after Effective Lifetime	06-Oct-21	7.8	A vulnerability in the proxy service of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to exhaust system memory and cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper memory management in the proxy service of an affected device. An attacker could exploit this vulnerability by establishing a large number of HTTPS connections to the affected device. A successful exploit could allow the attacker to cause the system to stop processing new connections, which could result in a DoS condition. Note: Manual intervention may be required to recover from this situation. **CVE ID : CVE-2021-34698**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-dos-fmHdKswk	H-CIS-WEB_-201021/585
web_security_appliance_s690x					
Missing Release of	06-Oct-21	7.8	A vulnerability in the proxy service of Cisco AsyncOS	https://tools.cisco.com/sec	H-CIS-WEB_-201021/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to exhaust system memory and cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper memory management in the proxy service of an affected device. An attacker could exploit this vulnerability by establishing a large number of HTTPS connections to the affected device. A successful exploit could allow the attacker to cause the system to stop processing new connections, which could result in a DoS condition. Note: Manual intervention may be required to recover from this situation. **CVE ID : CVE-2021-34698**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-dos-fmHdKswk	
wireless_ip_phone_8821					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	H-CIS-WIRE-201021/587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**		
Dell					
isilon_insightiq					
Use of a Broken or Risky Cryptographic Algorithm	01-Oct-21	7.5	Dell EMC InsightIQ, versions prior to 4.1.4, contain risky cryptographic algorithms in the SSH component. A remote unauthenticated attacker could potentially exploit this vulnerability leading to authentication bypass and remote takeover of the InsightIQ. This allows an attacker to take complete control of InsightIQ to affect services provided by SSH; so Dell recommends customers to upgrade at the earliest opportunity. **CVE ID : CVE-2021-36298**	https://www.dell.com/support/kbdoc/000191604	H-DEL-ISIL-201021/588
Digi					
6350-sr					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-6350-201021/589
Improper Authenticati	08-Oct-21	6.8	An issue was discovered in Digi RealPort through	N/A	H-DIG-6350-201021/590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**		
cm					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-CM-201021/591
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-CM-201021/592
connectcore_8x					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-CONN-201021/593
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-	N/A	H-DIG-CONN-201021/594

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
			in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**		
connectport_lts_8\\/16\\/32					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-CONN-201021/595
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-CONN-201021/596
connectport_ts_8\\/16					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-CONN-201021/597
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform	N/A	H-DIG-CONN-201021/598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication. **CVE ID : CVE-2021-35979**		
connect_es					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-CONN-201021/599
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-CONN-201021/600
one_ia					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-ONE_-201021/601
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication.	N/A	H-DIG-ONE_-201021/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35979		
one_iap_family					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-ONE_-201021/603
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-ONE_-201021/604
passport_integrated_console_server					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-PASS-201021/605
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-PASS-201021/606

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
portserver_ts					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-PORT-201021/607
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-PORT-201021/608
portserver_ts_mei					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-PORT-201021/609
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-PORT-201021/610
portserver_ts_mei_hardened					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-PORT-201021/611
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-PORT-201021/612
portserver_ts_m_mei					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-PORT-201021/613
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-PORT-201021/614
portserver_ts_p_mei					
Buffer Copy without	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows	N/A	H-DIG-PORT-201021/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**		
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-PORT-201021/616
transport_wr11_xt					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-TRAN-201021/617
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-TRAN-201021/618
wr21					
Buffer Copy without Checking Size of Input	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the	N/A	H-DIG-WR21-201021/619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**		
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-WR21-201021/620
wr31					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	H-DIG-WR31-201021/621
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-WR31-201021/622
wr44_r					
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response	N/A	H-DIG-WR44-201021/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**		
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	H-DIG-WR44-201021/624
IBM					
powervm_hypervisor					
N/A	06-Oct-21	6.5	IBM PowerVM Hypervisor FW1010 could allow a privileged user to gain access to another VM due to assigning duplicate WWPNs. IBM X-Force ID: 210162. **CVE ID : CVE-2021-38923**	https://exchange.xforce.ibmcloud.com/vulnerabilities/210162, https://www.ibm.com/support/pages/node/6495879	H-IBM-POWE-201021/625
ts7700					
Improper Authentication	06-Oct-21	10	The IBM TS7700 Management Interface is vulnerable to unauthenticated access. By accessing a specially-crafted URL, an attacker may gain administrative access to the Management Interface without authentication. IBM X-Force ID: 207747. **CVE ID : CVE-2021-29908**	https://www.ibm.com/support/pages/node/6495469, https://exchange.xforce.ibmcloud.com/vulnerabilities/207747	H-IBM-TS77-201021/626
mediatek					
mt6762					

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
Double Free	06-Oct-21	4	An improper error handling in Mediatek RRC Protocol stack prior to SMR Oct-2021 Release 1 allows modem crash and remote denial of service. **CVE ID : CVE-2021-25477**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-MED-MT67-201021/627
mt6765					
Double Free	06-Oct-21	4	An improper error handling in Mediatek RRC Protocol stack prior to SMR Oct-2021 Release 1 allows modem crash and remote denial of service. **CVE ID : CVE-2021-25477**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-MED-MT67-201021/628
mt6853					
Double Free	06-Oct-21	4	An improper error handling in Mediatek RRC Protocol stack prior to SMR Oct-2021 Release 1 allows modem crash and remote denial of service. **CVE ID : CVE-2021-25477**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-MED-MT68-201021/629
Mitsubishielectric					
got2000_gt2103-pmbd					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	H-MIT-GOT2-201021/630

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, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**		
got2000_gt2104-pmbd					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	H-MIT-GOT2-201021/631
got2000_gt2104-rtbd					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	H-MIT-GOT2-201021/632

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
			GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**		
got2000_gt2107-wtbd					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	H-MIT-GOT2-201021/633

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
got2000_gt2107-wtsd					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	H-MIT-GOT2-201021/634
got_simple_gs2107-wtbd					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	H-MIT-GOT_-201021/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**		
got_simple_gs2107-wtbd-n					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	H-MIT-GOT_-201021/636
got_simple_gs2110-wtbd					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	H-MIT-GOT_-201021/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**		
got_simple_gs2110-wtbd-n					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	H-MIT-GOT_-201021/638
le7-40gu-l					
Improper Handling of	07-Oct-21	5	Improper Handling of Exceptional Conditions	https://www.mitsubishiele	H-MIT-LE7--201021/639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**	ctric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	
r12ccpu-v					
Uncontrolled Resource Consumption	08-Oct-21	4.3	Uncontrolled resource consumption in MELSEC iQ-R series C Controller Module R12CCPU-V all versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending a large number of packets in a short time while the module starting up. **CVE ID : CVE-2021-20600**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-015_en.pdf	H-MIT-R12C-201021/640
Polycom					
vvx_400					
Improper Privilege Management	04-Oct-21	6.5	Polycom VVX 400/410 version 5.3.1 allows low-privileged users to change the Admin account	https://support.polycom.com/content/su	H-POL-VVX_-201021/641

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
			password by modifying a POST parameter name during the password reset process. **CVE ID : CVE-2021-41322**	pport.html	
vvx_410					
Improper Privilege Management	04-Oct-21	6.5	Polycom VVX 400/410 version 5.3.1 allows low-privileged users to change the Admin account password by modifying a POST parameter name during the password reset process. **CVE ID : CVE-2021-41322**	https://support.polycom.com/content/support.html	H-POL-VVX_-201021/642
ptcl					
hg150-ub					
Improper Authentication	04-Oct-21	7.5	An issue in the administrator authentication panel of PTCL HG150-Ub v3.0 allows attackers to bypass authentication via modification of the cookie value and Response Path. **CVE ID : CVE-2021-35296**	N/A	H-PTC-HG15-201021/643
Qnap					
nas					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	3.5	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Image2PDF. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this	https://www.qnap.com/en/security-advisory/qsa-21-43	H-QNA-NAS-201021/644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the following versions of Image2PDF: Image2PDF 2.1.5 (2021/08/17) and later **CVE ID : CVE-2021-38675**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	3.5	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Photo Station. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Photo Station: Photo Station 6.0.18 (2021/09/01) and later **CVE ID : CVE-2021-34354**	https://www.qnap.com/en/security-advisory/qsa-21-41	H-QNA-NAS-201021/645
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	3.5	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP NAS running Photo Station. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Photo Station: Photo Station 5.4.10 (2021/08/19) and later Photo Station 5.7.13 (2021/08/19) and later Photo Station 6.0.18 (2021/09/01) and later **CVE ID : CVE-2021-34355**	https://www.qnap.com/en/security-advisory/qsa-21-42	H-QNA-NAS-201021/646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-21	3.5	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Photo Station. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Photo Station: Photo Station 6.0.18 (2021/09/01) and later **CVE ID : CVE-2021-34356**	https://www.qnap.com/en/security-advisory/qsa-21-41	H-QNA-NAS-201021/647
Qualcomm					
qualcomm					
Authentication Bypass by Capture-replay	06-Oct-21	5	A lack of replay attack protection in GUTI REALLOCATION COMMAND message process in Qualcomm modem prior to SMR Oct-2021 Release 1 can lead to remote denial of service on mobile network connection. **CVE ID : CVE-2021-25480**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-QUA-QUAL-201021/648
Samsung					
exynos					
Improper Input Validation	06-Oct-21	2.1	A possible guessing and confirming a byte memory vulnerability in Widevine trustlet prior to SMR Oct-2021 Release 1 allows attackers to read arbitrary memory address. **CVE ID : CVE-2021-25468**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/649

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
Out-of-bounds Write	06-Oct-21	4.6	A possible stack-based buffer overflow vulnerability in Widevine trustlet prior to SMR Oct-2021 Release 1 allows arbitrary code execution. **CVE ID : CVE-2021-25469**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/650
Incorrect Authorization	06-Oct-21	3.6	An improper caller check logic of SMC call in TEEGRIS secure OS prior to SMR Oct-2021 Release 1 can be used to compromise TEE. **CVE ID : CVE-2021-25470**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/651
N/A	06-Oct-21	5	A lack of replay attack protection in Security Mode Command process prior to SMR Oct-2021 Release 1 can lead to denial of service on mobile network connection and battery depletion. **CVE ID : CVE-2021-25471**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/652
Incorrect Authorization	06-Oct-21	2.1	An information disclosure vulnerability in Widevine TA log prior to SMR Oct-2021 Release 1 allows attackers to bypass the ASLR protection mechanism in TEE. **CVE ID : CVE-2021-25476**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/653
Out-of-bounds Write	06-Oct-21	6.5	A possible stack-based buffer overflow vulnerability in Exynos CP Chipset prior to SMR Oct-2021 Release 1 allows arbitrary memory write and code execution.	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/654

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-2021-25478		
Out-of-bounds Write	06-Oct-21	6.5	A possible heap-based buffer overflow vulnerability in Exynos CP Chipset prior to SMR Oct-2021 Release 1 allows arbitrary memory write and code execution. **CVE ID : CVE-2021-25479**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/655
Improper Check for Unusual or Exceptional Conditions	06-Oct-21	4.6	An improper error handling in Exynos CP booting driver prior to SMR Oct-2021 Release 1 allows local attackers to bypass a Secure Memory Protector of Exynos CP Memory. **CVE ID : CVE-2021-25481**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/656
Out-of-bounds Read	06-Oct-21	4.6	Lack of boundary checking of a buffer in set_skb_priv() of modem interface driver prior to SMR Oct-2021 Release 1 allows OOB read and it results in arbitrary code execution by dereference of invalid function pointer. **CVE ID : CVE-2021-25487**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/657
Out-of-bounds Read	06-Oct-21	2.1	Lack of boundary checking of a buffer in recv_data() of modem interface driver prior to SMR Oct-2021 Release 1 allows OOB read. **CVE ID : CVE-2021-25488**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/658
Improper Input Validation	06-Oct-21	4.9	Assuming radio permission is gained, missing input validation in modem interface driver prior to	https://security.samsungmobile.com/securityUpdate.s	H-SAM-EXYN-201021/659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMR Oct-2021 Release 1 results in format string bug leading to kernel panic. **CVE ID : CVE-2021-25489**	msb?year=2021&month=10	
NULL Pointer Dereference	06-Oct-21	2.1	A vulnerability in mfc driver prior to SMR Oct-2021 Release 1 allows memory corruption via NULL-pointer dereference. **CVE ID : CVE-2021-25491**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/660
exynos_2100					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.2	Assuming system privilege is gained, possible buffer overflow vulnerabilities in the Vision DSP kernel driver prior to SMR Oct-2021 Release 1 allows privilege escalation to Root by hijacking loaded library. **CVE ID : CVE-2021-25467**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/661
Out-of-bounds Write	06-Oct-21	7.2	A possible heap-based buffer overflow vulnerability in DSP kernel driver prior to SMR Oct-2021 Release 1 allows arbitrary memory write and code execution. **CVE ID : CVE-2021-25475**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/662
exynos_980					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.2	Assuming system privilege is gained, possible buffer overflow vulnerabilities in the Vision DSP kernel driver prior to SMR Oct-2021 Release 1 allows privilege escalation to Root by hijacking loaded library.	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/663

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
			CVE ID : CVE-2021-25467		
Out-of-bounds Write	06-Oct-21	7.2	A possible heap-based buffer overflow vulnerability in DSP kernel driver prior to SMR Oct-2021 Release 1 allows arbitrary memory write and code execution. **CVE ID : CVE-2021-25475**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/664
exynos_9830					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.2	Assuming system privilege is gained, possible buffer overflow vulnerabilities in the Vision DSP kernel driver prior to SMR Oct-2021 Release 1 allows privilege escalation to Root by hijacking loaded library. **CVE ID : CVE-2021-25467**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/665
Out-of-bounds Write	06-Oct-21	7.2	A possible heap-based buffer overflow vulnerability in DSP kernel driver prior to SMR Oct-2021 Release 1 allows arbitrary memory write and code execution. **CVE ID : CVE-2021-25475**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	H-SAM-EXYN-201021/666
visual-tools					
dvr_vx16					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Oct-21	10	In Visual Tools DVR VX16 4.2.28.0, an unauthenticated attacker can achieve remote command execution via shell metacharacters in the cgi-bin/slogin/login.py User-Agent HTTP header.	https://visual-tools.com/	H-VIS-DVR_-201021/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-42071		
Operating System					
Apple					
macos					
Incorrect Permission Assignment for Critical Resource	01-Oct-21	4.6	The MacOS version of Multipass, version 1.7.0, fixed in 1.7.2, accidentally installed the application directory with incorrect owner. **CVE ID : CVE-2021-3747**	https://github.com/canonical/multipass/issues/2261	O-APP-MACO-201021/668
Use After Free	07-Oct-21	6.8	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability when processing AcroForm listbox that could result in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **CVE ID : CVE-2021-40725**	https://helpx.adobe.com/security/products/acrobat/apsb21-55.html	O-APP-MACO-201021/669
Use After Free	07-Oct-21	6.8	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability	https://helpx.adobe.com/security/products/acrobat/apsb21-55.html	O-APP-MACO-201021/670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when processing AcroForm field that could result in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **CVE ID : CVE-2021-40726**		
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVRDL unpacking module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-40832**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40832	O-APP-MACO-201021/671
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVPACK module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-	O-APP-MACO-201021/672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33603**	secure.com/en/business/support-and-downloads/security-advisories/cve-2021-33603	
Time-of-check Time-of-use (TOCTOU) Race Condition	06-Oct-21	6.9	A vulnerability in the shared library loading mechanism of Cisco AnyConnect Secure Mobility Client for Linux and Mac OS could allow an authenticated, local attacker to perform a shared library hijacking attack on an affected device if the VPN Posture (HostScan) Module is installed on the AnyConnect client. This vulnerability is due to a race condition in the signature verification process for shared library files that are loaded on an affected device. An attacker could exploit this vulnerability by sending a series of crafted interprocess communication (IPC) messages to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected device with root privileges. To exploit this vulnerability, the attacker must have a valid	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-lib-hija-cAFB7x4q	O-APP-MACO-201021/673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			account on the system. **CVE ID : CVE-2021-34788**		
Axis					
axis_os					
Out-of-bounds Write	05-Oct-21	4	User controlled parameters related to SMTP notifications are not correctly validated. This can lead to a buffer overflow resulting in crashes and data leakage. **CVE ID : CVE-2021-31986**	https://www.axis.com/files/tech_notes/CVE-2021-31986.pdf	O-AXI-AXIS-201021/674
Improper Input Validation	05-Oct-21	5.1	A user controlled parameter related to SMTP test functionality is not correctly validated making it possible to bypass blocked network recipients. **CVE ID : CVE-2021-31987**	https://www.axis.com/files/tech_notes/CVE-2021-31987.pdf	O-AXI-AXIS-201021/675
Improper Input Validation	05-Oct-21	6.8	A user controlled parameter related to SMTP test functionality is not correctly validated making it possible to add the Carriage Return and Line Feed (CRLF) control characters and include arbitrary SMTP headers in the generated test email. **CVE ID : CVE-2021-31988**	https://www.axis.com/files/tech_notes/CVE-2021-31988.pdf	O-AXI-AXIS-201021/676
axis_os_2016					
Out-of-bounds Write	05-Oct-21	4	User controlled parameters related to SMTP notifications are not correctly validated. This can lead to a buffer overflow resulting in	https://www.axis.com/files/tech_notes/CVE-2021-31986.pdf	O-AXI-AXIS-201021/677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crashes and data leakage. **CVE ID : CVE-2021-31986**		
Improper Input Validation	05-Oct-21	5.1	A user controlled parameter related to SMTP test functionality is not correctly validated making it possible to bypass blocked network recipients. **CVE ID : CVE-2021-31987**	https://www.axis.com/files/tech_notes/CVE-2021-31987.pdf	O-AXI-AXIS-201021/678
Improper Input Validation	05-Oct-21	6.8	A user controlled parameter related to SMTP test functionality is not correctly validated making it possible to add the Carriage Return and Line Feed (CRLF) control characters and include arbitrary SMTP headers in the generated test email. **CVE ID : CVE-2021-31988**	https://www.axis.com/files/tech_notes/CVE-2021-31988.pdf	O-AXI-AXIS-201021/679
axis_os_2018					
Out-of-bounds Write	05-Oct-21	4	User controlled parameters related to SMTP notifications are not correctly validated. This can lead to a buffer overflow resulting in crashes and data leakage. **CVE ID : CVE-2021-31986**	https://www.axis.com/files/tech_notes/CVE-2021-31986.pdf	O-AXI-AXIS-201021/680
Improper Input Validation	05-Oct-21	5.1	A user controlled parameter related to SMTP test functionality is not correctly validated making it possible to bypass blocked network recipients. **CVE ID : CVE-2021-31987**	https://www.axis.com/files/tech_notes/CVE-2021-31987.pdf	O-AXI-AXIS-201021/681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-Oct-21	6.8	A user controlled parameter related to SMTP test functionality is not correctly validated making it possible to add the Carriage Return and Line Feed (CRLF) control characters and include arbitrary SMTP headers in the generated test email. **CVE ID : CVE-2021-31988**	https://www.axis.com/files/tech_notes/CVE-2021-31988.pdf	O-AXI-AXIS-201021/682
axis_os_2020					
Out-of-bounds Write	05-Oct-21	4	User controlled parameters related to SMTP notifications are not correctly validated. This can lead to a buffer overflow resulting in crashes and data leakage. **CVE ID : CVE-2021-31986**	https://www.axis.com/files/tech_notes/CVE-2021-31986.pdf	O-AXI-AXIS-201021/683
Improper Input Validation	05-Oct-21	5.1	A user controlled parameter related to SMTP test functionality is not correctly validated making it possible to bypass blocked network recipients. **CVE ID : CVE-2021-31987**	https://www.axis.com/files/tech_notes/CVE-2021-31987.pdf	O-AXI-AXIS-201021/684
Improper Input Validation	05-Oct-21	6.8	A user controlled parameter related to SMTP test functionality is not correctly validated making it possible to add the Carriage Return and Line Feed (CRLF) control characters and include arbitrary SMTP headers in the generated test email.	https://www.axis.com/files/tech_notes/CVE-2021-31988.pdf	O-AXI-AXIS-201021/685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31988		
bosch					
indracontrol_xlc_firmware					
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-INDR-201021/686
rexroth_indramotion_mlc_firmware					
Use of Password Hash With Insufficient Computational Effort	04-Oct-21	5	The user and password data base is exposed by an unprotected web server resource. Passwords are hashed with a weak hashing algorithm and therefore allow an attacker to determine the password by using rainbow tables. **CVE ID : CVE-2021-23855**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/687
rexroth_indramotion_mlc_l20_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-21	4.3	The web server is vulnerable to reflected XSS and therefore an attacker might be able to execute scripts on a client's computer by sending the client a manipulated URL. **CVE ID : CVE-2021-23856**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/688

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 Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/689
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/690
rexroth_indramotion_mlc_l25_firmware					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/691
Insufficiently	04-Oct-21	7.8	Information disclosure:	https://psirt.	O-BOS-REXR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	bosch.com/security-advisories/bosch-sa-741752.html	201021/692
rexroth_indramotion_mlc_l40_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Oct-21	4.3	The web server is vulnerable to reflected XSS and therefore an attacker might be able to execute scripts on a client's computer by sending the client a manipulated URL. **CVE ID : CVE-2021-23856**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/693
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/694
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected	https://psirt.bosch.com/security-advisories/bosch-sa-	O-BOS-REXR-201021/695

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
			web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	741752.html	
rexroth_indramotion_mlc_l45_firmware					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/696
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/697
rexroth_indramotion_mlc_l65_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/698
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/699
rexroth_indramotion_mlc_l75_firmware					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/700
Insufficiently	04-Oct-21	7.8	Information disclosure:	https://psirt.	O-BOS-REXR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	bosch.com/security-advisories/bosch-sa-741752.html	201021/701
rexroth_indramotion_mlc_l85_firmware					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/702
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/703

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
			server resource. **CVE ID : CVE-2021-23858**		
rexroth_indramotion_mlc_xm21_firmware					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/704
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/705
rexroth_indramotion_mlc_xm22_firmware					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/706

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
			subsequently login to the system. **CVE ID : CVE-2021-23857**		
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/707
rexroth_indramotion_mlc_xm41_firmware					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/708
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/709

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
			are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**		
rexroth_indramotion_mlc_xm42_firmware					
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/710
Insufficiently Protected Credentials	04-Oct-21	7.8	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource. **CVE ID : CVE-2021-23858**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/711
rexroth_indramotion_xlc_firmware					
Use of Password Hash With Insufficient	04-Oct-21	5	The user and password data base is exposed by an unprotected web server resource. Passwords are	https://psirt.bosch.com/security-advisories/bo	O-BOS-REXR-201021/712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Computational Effort			hashed with a weak hashing algorithm and therefore allow an attacker to determine the password by using rainbow tables. **CVE ID : CVE-2021-23855**	sch-sa-741752.html	
Improper Authentication	04-Oct-21	10	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system. **CVE ID : CVE-2021-23857**	https://psirt.bosch.com/security-advisories/bosch-sa-741752.html	O-BOS-REXR-201021/713
bostonscientific					
zoom_latitude_pogrammer\\/recorder\\/monitor_3120_firmware					
Improper Access Control	04-Oct-21	7.2	A skilled attacker with physical access to the affected device can gain access to the hard disk drive of the device to change the telemetry region and could use this setting to interrogate or program an implantable device in any region in the world. **CVE ID : CVE-2021-38392**	N/A	O-BOS-ZOOM-201021/714
Missing Protection Against Hardware Reverse Engineering Using	04-Oct-21	6.9	An attacker with physical access to the device can extract the binary that checks for the hardware key and reverse engineer it, which could be used to create a physical duplicate	N/A	O-BOS-ZOOM-201021/715

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
Integrated Circuit (IC) Imaging Techniques			of a valid hardware key. The hardware key allows access to special settings when inserted. **CVE ID : CVE-2021-38394**		
Insufficient Verification of Data Authenticity	04-Oct-21	4.6	The programmer installation utility does not perform a cryptographic authenticity or integrity checks of the software on the flash drive. An attacker could leverage this weakness to install unauthorized software using a specially crafted USB. **CVE ID : CVE-2021-38396**	N/A	O-BOS-ZOOM-201021/716
N/A	04-Oct-21	4.6	The affected device uses off-the-shelf software components that contain unpatched vulnerabilities. A malicious attacker with physical access to the affected device could exploit these vulnerabilities. **CVE ID : CVE-2021-38398**	N/A	O-BOS-ZOOM-201021/717
Use of Password Hash With Insufficient Computational Effort	04-Oct-21	4.6	An attacker with physical access to Boston Scientific Zoom Latitude Model 3120 can remove the hard disk drive or create a specially crafted USB to extract the password hash for brute force reverse engineering of the system password. **CVE ID : CVE-2021-38400**	N/A	O-BOS-ZOOM-201021/718
zoom_latitude_programming_system_model_3120_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Oct-21	4.6	The affected device uses off-the-shelf software components that contain unpatched vulnerabilities. A malicious attacker with physical access to the affected device could exploit these vulnerabilities. **CVE ID : CVE-2021-38398**	N/A	O-BOS-ZOOM-201021/719
Canonical					
ubuntu_linux					
Exposure of Resource to Wrong Sphere	01-Oct-21	2.1	Function check_attachment_for_errors() in file data/general-hooks/ubuntu.py could be tricked into exposing private data via a constructed crash file. This issue affects: apport 2.14.1 versions prior to 2.14.1-0ubuntu3.29+esm8; 2.20.1 versions prior to 2.20.1-0ubuntu2.30+esm2; 2.20.9 versions prior to 2.20.9-0ubuntu7.26; 2.20.11 versions prior to 2.20.11-0ubuntu27.20; 2.20.11 versions prior to 2.20.11-0ubuntu65.3; **CVE ID : CVE-2021-3709**	https://bugs.launchpad.net/ubuntu/+source/apport/+bug/1934308, https://ubuntu.com/security/notices/USN-5077-1, https://ubuntu.com/security/notices/USN-5077-2	O-CAN-UBUN-201021/720
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Oct-21	4.7	An information disclosure via path traversal was discovered in apport/hookutils.py function read_file(). This issue affects: apport 2.14.1 versions prior to 2.14.1-0ubuntu3.29+esm8; 2.20.1	https://ubuntu.com/security/notices/USN-5077-1, https://ubuntu.com/security/notices/USN-5077-2,	O-CAN-UBUN-201021/721

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 prior to 2.20.1-0ubuntu2.30+esm2; 2.20.9 versions prior to 2.20.9-0ubuntu7.26; 2.20.11 versions prior to 2.20.11-0ubuntu27.20; 2.20.11 versions prior to 2.20.11-0ubuntu65.3; **CVE ID : CVE-2021-3710**	https://bugs.launchpad.net/ubuntu/+source/apport/+bug/1933832	
Cisco					
asyncos					
N/A	06-Oct-21	5	A vulnerability in the antispam protection mechanisms of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2021-1534**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-sGcfsDrp	O-CIS-ASYN-201021/722
Missing Release of Memory after	06-Oct-21	7.8	A vulnerability in the proxy service of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could	https://tools.cisco.com/security/center/content/Cisco	O-CIS-ASYN-201021/723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			allow an unauthenticated, remote attacker to exhaust system memory and cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper memory management in the proxy service of an affected device. An attacker could exploit this vulnerability by establishing a large number of HTTPS connections to the affected device. A successful exploit could allow the attacker to cause the system to stop processing new connections, which could result in a DoS condition. Note: Manual intervention may be required to recover from this situation. **CVE ID : CVE-2021-34698**	SecurityAdvisory/cisco-sa-wsa-dos-fmHdKswk	
ata_190_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	9	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34710**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-A4J57F3	O-CIS-ATA_-201021/724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	7.8	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34735**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-A4J57F3	O-CIS-ATA_-201021/725
ata_191_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	9	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34710**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-A4J57F3	O-CIS-ATA_-201021/726
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	7.8	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-	O-CIS-ATA_-201021/727

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 service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34735**	A4J57F3	
ata_192_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	9	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34710**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-A4J57F3	O-CIS-ATA_-201021/728
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-21	7.8	Multiple vulnerabilities in the Cisco ATA 190 Series Analog Telephone Adapter Software could allow an attacker to perform a command injection attack resulting in remote code execution or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34735**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-A4J57F3	O-CIS-ATA_-201021/729
business_220-16p-2g_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/730
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/731
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/732

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
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/734
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/737
business_220-16t-2g_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/738
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/739
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/740

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
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/742
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/744

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/745
business_220-24fp-4g_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/746
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/747
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/748

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
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/750
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/752

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/753
business_220-24fp-4x_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/754
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/755
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/758
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/759

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
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/761
business_220-24p-4g_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
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/762
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/763
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/764

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
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/766
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/769
business_220-24p-4x_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/770
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/771
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/774
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/777
business_220-24t-4g_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/778
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/779
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/780

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
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/782
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/785
business_220-24t-4x_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/786
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/787
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/788

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
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/790
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/791

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
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/793
business_220-48fp-4x_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/794
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/795
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/796

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
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/798
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/801
business_220-48p-4g_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/802
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/803
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/805

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
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/806
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/809
business_220-48p-4x_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/810
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/811
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/812

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
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/813

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 affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/814
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/816

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/817
business_220-48t-4g_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/818
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/819
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/820

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
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/822
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/824

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/825
business_220-48t-4x_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/826
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/827
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/828

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
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/830
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/832

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/833
business_220-8fp-e-2g_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/834
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/835
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/838
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/841
business_220-8p-e-2g_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/842
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/843
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/846
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/848

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
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/849
business_220-8t-e-2g_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	4	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34744**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/850
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-21	3.6	Multiple vulnerabilities in Cisco Business 220 Series Smart Switches firmware could allow an attacker with Administrator privileges to access sensitive login credentials or reconfigure the passwords on the user account. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34757**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX	O-CIS-BUSI-201021/851
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/852

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
			it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34775**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/853

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 affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34776**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34777**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/854
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Oct-21	2.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-BUSI-201021/855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34778**	sb220-lldp-multivuls-mVRUtQ8T	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-21	7.9	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches. An unauthenticated, adjacent attacker could perform the following: Execute code on the affected device or cause it to reload unexpectedly Cause LLDP database corruption on the affected device For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released firmware updates that address these vulnerabilities. **CVE ID : CVE-2021-34780**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T	O-CIS-BUSI-201021/857
ip_conference_phone_7832_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
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	O-CIS-IP_C-201021/858
ip_conference_phone_8832_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	O-CIS-IP_C-201021/859
ip_phones_8832_firmware					
Improper	06-Oct-21	2.1	A vulnerability in the debug	https://tools.	O-CIS-IP_P-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	201021/860
ip_phone_7811_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	O-CIS-IP_P-201021/861
ip_phone_7821_firmware					
Improper Limitation of	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone	https://tools.cisco.com/sec	O-CIS-IP_P-201021/862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	urity/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	
ip_phone_7832_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	O-CIS-IP_P-201021/863
ip_phone_7841_firmware					
Improper Limitation of a Pathname	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an	https://tools.cisco.com/security/center/	O-CIS-IP_P-201021/864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	
ip_phone_7861_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	O-CIS-IP_P-201021/865
ip_phone_8811_firmware					
Improper Limitation of a Pathname to a	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201021/866

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
Restricted Directory ('Path Traversal')			attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	SecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	
ip_phone_8831_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	O-CIS-IP_P-201021/867
ip_phone_8841_firmware					
Improper Limitation of a Pathname to a Restricted	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on	https://tools.cisco.com/security/center/content/CiscoSecurityAdvis	O-CIS-IP_P-201021/868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	ory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	
ip_phone_8845_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	O-CIS-IP_P-201021/869
ip_phone_8851_firmware					
Improper Limitation of a Pathname to a Restricted Directory	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_P-201021/870

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
('Path Traversal')			vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	ipphone-arbfileread-NPdtE2Ow	
ip_phone_8861_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	O-CIS-IP_P-201021/871
ip_phone_8865_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-	O-CIS-IP_P-201021/872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	arbfileread-NPdtE2Ow	
roomos					
Incorrect Permission Assignment for Critical Resource	06-Oct-21	2.1	A vulnerability in the memory management of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an authenticated, local attacker to corrupt a shared memory segment, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient access controls to a shared memory resource. An attacker could exploit this vulnerability by corrupting a shared memory segment on an affected device. A successful exploit could allow the attacker to cause the device to reload. The device will recover from the corruption upon reboot. **CVE ID : CVE-2021-34758**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tpce-rmos-mem-dos-rck56tT	O-CIS-ROOM-201021/873
wireless_ip_phone_8821_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
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-21	2.1	A vulnerability in the debug shell of Cisco IP Phone software could allow an authenticated, local attacker to read any file on the device file system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by providing crafted input to a debug shell command. A successful exploit could allow the attacker to read any file on the device file system. **CVE ID : CVE-2021-34711**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow	O-CIS-WIRE-201021/874
Debian					
debian_linux					
Improper Input Validation	08-Oct-21	4.6	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In versions prior to 1.10.4 and 1.12.0, Flatpak apps with direct access to AF_UNIX sockets such as those used by Wayland, Pipewire or pipewire-pulse can trick portals and other host-OS services into treating the Flatpak app as though it was an ordinary, non-sandboxed host-OS process. They can do this by manipulating the VFS using recent mount-related syscalls that are not blocked by Flatpak's	https://github.com/flatpak/flatpak/commit/1330662f33a55e88bfe18e76de28b7922d91a999, https://github.com/flatpak/flatpak/commit/a10f52a7565c549612c92b8e736a6698a53db330, https://github.com/flatpak/flatpak/commit/4c34815784e9ffda5733225c7d9582	O-DEB-DEBI-201021/875

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
			denylist seccomp filter, in order to substitute a crafted `/.flatpak-info` or make that file disappear entirely. Flatpak apps that act as clients for AF_UNIX sockets such as those used by Wayland, Pipewire or pipewire-pulse can escalate the privileges that the corresponding services will believe the Flatpak app has. Note that protocols that operate entirely over the D-Bus session bus (user bus), system bus or accessibility bus are not affected by this. This is due to the use of a proxy process `xdg-dbus-proxy`, whose VFS cannot be manipulated by the Flatpak app, when interacting with these buses. Patches exist for versions 1.10.4 and 1.12.0, and as of time of publication, a patch for version 1.8.2 is being planned. There are no workarounds aside from upgrading to a patched version. **CVE ID : CVE-2021-41133**	4f96375e36	
Dell					
enterprise_sonic_os					
Exposure of Sensitive Information to an Unauthorize	01-Oct-21	4	Dell Enterprise SONiC OS, versions 3.3.0 and earlier, contains a sensitive information disclosure vulnerability. An	https://www.dell.com/support/kbdoc/en-us/00019169	O-DEL-ENTE-201021/876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Actor			authenticated malicious user with access to the system may use the TACACS\Radius credentials stored to read sensitive information and use it in further attacks. **CVE ID : CVE-2021-36309**	0/DSA-2021-190-Dell-Enterprise-SONiC-OS-Security-Update-for-an-information-disclosure-Vulnerability	
isilon_insightiq_firmware					
Use of a Broken or Risky Cryptographic Algorithm	01-Oct-21	7.5	Dell EMC InsightIQ, versions prior to 4.1.4, contain risky cryptographic algorithms in the SSH component. A remote unauthenticated attacker could potentially exploit this vulnerability leading to authentication bypass and remote takeover of the InsightIQ. This allows an attacker to take complete control of InsightIQ to affect services provided by SSH; so Dell recommends customers to upgrade at the earliest opportunity. **CVE ID : CVE-2021-36298**	https://www.dell.com/support/kbdoc/000191604	O-DEL-ISIL-201021/877
Digi					
6350-sr_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution.	N/A	O-DIG-6350-201021/878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35977		
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-6350-201021/879
cm_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-CM_F-201021/880
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-CM_F-201021/881
connectcore_8x_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-CONN-201021/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-CONN-201021/883
connectport_lts_8\\/16\\/32_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-CONN-201021/884
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-CONN-201021/885
connectport_ts_8\\/16_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-CONN-201021/886
Improper Authenticati	08-Oct-21	6.8	An issue was discovered in Digi RealPort through	N/A	O-DIG-CONN-201021/887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**		
connect_es_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-CONN-201021/888
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-CONN-201021/889
one_iap_family_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-ONE_-201021/890
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-	N/A	O-DIG-ONE_-201021/891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**		
one_ia_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-ONE_-201021/892
Improper Authenticati on	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-ONE_-201021/893
passport_integrated_console_server_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-PASS-201021/894
Improper Authenticati on	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform	N/A	O-DIG-PASS-201021/895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication. **CVE ID : CVE-2021-35979**		
portserver_ts_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-PORT-201021/896
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-PORT-201021/897
portserver_ts_mei_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-PORT-201021/898
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication.	N/A	O-DIG-PORT-201021/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35979		
portserver_ts_mei_hardened_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-PORT-201021/900
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-PORT-201021/901
portserver_ts_m_mei_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-PORT-201021/902
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-PORT-201021/903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
portserver_ts_p_mei_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-PORT-201021/904
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-PORT-201021/905
transport_wr11_xt_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-TRAN-201021/906
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-TRAN-201021/907
wr21_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-WR21-201021/908
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-WR21-201021/909
wr31_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**	N/A	O-DIG-WR31-201021/910
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-WR31-201021/911
wr44_r_firmware					
Buffer Copy without	08-Oct-21	7.5	An issue was discovered in Digi RealPort for Windows	N/A	O-DIG-WR44-201021/912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution. **CVE ID : CVE-2021-35977**		
Improper Authentication	08-Oct-21	6.8	An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication. **CVE ID : CVE-2021-35979**	N/A	O-DIG-WR44-201021/913
Fedoraproject					
fedora					
Use After Free	08-Oct-21	6.8	Use after free in Offline use in Google Chrome on Android prior to 94.0.4606.54 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37956**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1243117	O-FED-FEDO-201021/914
Use After Free	08-Oct-21	6.8	Use after free in WebGPU in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37957**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1242269	O-FED-FEDO-201021/915
N/A	08-Oct-21	5.8	Inappropriate	https://chro	O-FED-FEDO-

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
			implementation in Navigation in Google Chrome on Windows prior to 94.0.4606.54 allowed a remote attacker to inject scripts or HTML into a privileged page via a crafted HTML page. **CVE ID : CVE-2021-37958**	mereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1223290	201021/916
Use After Free	08-Oct-21	6.8	Use after free in Task Manager in Google Chrome prior to 94.0.4606.54 allowed an attacker who convinced a user to enage in a series of user gestures to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37959**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1229625	O-FED-FEDO-201021/917
Use After Free	08-Oct-21	6.8	Use after free in Tab Strip in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37961**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1228557	O-FED-FEDO-201021/918
Use After Free	08-Oct-21	6.8	Use after free in Performance Manager in Google Chrome prior to 94.0.4606.54 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37962**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1231933	O-FED-FEDO-201021/919

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-Oct-21	4.3	Side-channel information leakage in DevTools in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to bypass site isolation via a crafted HTML page. **CVE ID : CVE-2021-37963**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1199865	O-FED-FEDO-201021/920
N/A	08-Oct-21	4.3	Inappropriate implementation in ChromeOS Networking in Google Chrome on ChromeOS prior to 94.0.4606.54 allowed an attacker with a rogue wireless access point to to potentially carryout a wifi impersonation attack via a crafted ONC file. **CVE ID : CVE-2021-37964**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1203612	O-FED-FEDO-201021/921
Exposure of Resource to Wrong Sphere	08-Oct-21	4.3	Inappropriate implementation in Background Fetch API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-37965**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1239709	O-FED-FEDO-201021/922
Origin Validation Error	08-Oct-21	4.3	Inappropriate implementation in Compositing in Google Chrome on Android prior to 94.0.4606.54 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html,	O-FED-FEDO-201021/923

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
			crafted HTML page. **CVE ID : CVE-2021-37966**	https://crbug.com/1238944	
Exposure of Resource to Wrong Sphere	08-Oct-21	4.3	Inappropriate implementation in Background Fetch API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-37967**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1243622	O-FED-FEDO-201021/924
Exposure of Resource to Wrong Sphere	08-Oct-21	4.3	Inappropriate implementation in Background Fetch API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-37968**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1245053	O-FED-FEDO-201021/925
Improper Privilege Management	08-Oct-21	6.8	Inappropriate implementation in Google Updater in Google Chrome on Windows prior to 94.0.4606.54 allowed a remote attacker to perform local privilege escalation via a crafted file. **CVE ID : CVE-2021-37969**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1245879	O-FED-FEDO-201021/926
Use After Free	08-Oct-21	6.8	Use after free in File System API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-	O-FED-FEDO-201021/927

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
			corruption via a crafted HTML page. **CVE ID : CVE-2021-37970**	desktop_21.html, https://crbug.com/1248030	
Origin Validation Error	08-Oct-21	4.3	Incorrect security UI in Web Browser UI in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-37971**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1219354	O-FED-FEDO-201021/928
Out-of-bounds Read	08-Oct-21	6.8	Out of bounds read in libjpeg-turbo in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-37972**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1234259	O-FED-FEDO-201021/929
Use After Free	08-Oct-21	6.8	Use after free in Portals in Google Chrome prior to 94.0.4606.61 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2021-37973**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_24.html, https://crbug.com/1251727	O-FED-FEDO-201021/930
Integer Overflow or Wraparound	04-Oct-21	6	Redis is an open source, in-memory database that persists on disk. An integer overflow bug in the underlying string library can be used to corrupt the	https://github.com/redis/redis/commit/c6ad876774f3cc11e32681ea02a2eead0	O-FED-FEDO-201021/931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			heap and potentially result with denial of service or remote code execution. The vulnerability involves changing the default proto-max-bulk-len configuration parameter to a very large value and constructing specially crafted network payloads or commands. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the proto-max-bulk-len configuration parameter. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command. **CVE ID : CVE-2021-41099**	0f2c521, https://github.com/redis/redis/security/advisories/GHSA-j3cr-9h5g-6cph	
Improper Input Validation	08-Oct-21	4.6	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In versions prior to 1.10.4 and 1.12.0, Flatpak apps with direct access to AF_UNIX sockets such as those used by Wayland, Pipewire or pipewire-pulse can trick portals and other host-OS services into treating the Flatpak app as though it was an ordinary, non-sandboxed host-OS	https://github.com/flatpak/flatpak/commit/1330662f33a55e88bfe18e76de28b7922d91a999, https://github.com/flatpak/flatpak/commit/a10f52a7565c549612c92b8e736a6698a53db330, https://githu	O-FED-FEDO-201021/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			process. They can do this by manipulating the VFS using recent mount-related syscalls that are not blocked by Flatpak's denylist seccomp filter, in order to substitute a crafted `/.flatpak-info` or make that file disappear entirely. Flatpak apps that act as clients for AF_UNIX sockets such as those used by Wayland, Pipewire or pipewire-pulse can escalate the privileges that the corresponding services will believe the Flatpak app has. Note that protocols that operate entirely over the D-Bus session bus (user bus), system bus or accessibility bus are not affected by this. This is due to the use of a proxy process `xdg-dbus-proxy`, whose VFS cannot be manipulated by the Flatpak app, when interacting with these buses. Patches exist for versions 1.10.4 and 1.12.0, and as of time of publication, a patch for version 1.8.2 is being planned. There are no workarounds aside from upgrading to a patched version. **CVE ID : CVE-2021-41133**	b.com/flatpak/flatpak/commit/4c34815784e9ffda5733225c7d95824f96375e36	
NULL Pointer	05-Oct-21	5	While fuzzing the 2.4.49 httpd, a new null pointer	https://httpd.apache.org/se	O-FED-FEDO-201021/933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			dereference was detected during HTTP/2 request processing, allowing an external source to DoS the server. This requires a specially crafted request. The vulnerability was recently introduced in version 2.4.49. No exploit is known to the project. **CVE ID : CVE-2021-41524**	curity/vulnerabilities_24.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-21	4.3	MediaWiki before 1.36.2 allows XSS. Month related MediaWiki messages are not escaped before being used on the Special:Search results page. **CVE ID : CVE-2021-41798**	https://phabricator.wikimedia.org/T285515	O-FED-FEDO-201021/934
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Oct-21	7.5	It was found that the fix for CVE-2021-41773 in Apache HTTP Server 2.4.50 was insufficient. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue only affects Apache 2.4.49 and Apache 2.4.50 and not earlier versions.	https://httpd.apache.org/security/vulnerabilities_24.html, https://lists.apache.org/thread.html/r17a4c6ce9aff662efd9459e9d1850ab4a611cb23392fc68264c72cb3@%3Ccvs.httpd.apache.org%3E	O-FED-FEDO-201021/935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-42013		
Use After Free	08-Oct-21	6.8	Use after free in Selection API in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who convinced the user the visit a malicious website to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30625**	https://crbug.com/1237533 , https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	O-FED-FEDO-201021/936
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Oct-21	6.8	Out of bounds memory access in ANGLE in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30626**	https://crbug.com/1241036 , https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	O-FED-FEDO-201021/937
Access of Resource Using Incompatible Type ('Type Confusion')	08-Oct-21	6.8	Type confusion in Blink layout in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30627**	https://crbug.com/1245786 , https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	O-FED-FEDO-201021/938
Out-of-bounds Write	08-Oct-21	6.8	Stack buffer overflow in ANGLE in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page. **CVE ID : CVE-2021-30628**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html, https://crbug.	O-FED-FEDO-201021/939

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
				com/1241123	
Use After Free	08-Oct-21	6.8	Use after free in Permissions in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30629**	https://crbug.com/1243646 , https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	O-FED-FEDO-201021/940
Exposure of Resource to Wrong Sphere	08-Oct-21	4.3	Inappropriate implementation in Blink in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-30630**	https://crbug.com/1244568 , https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	O-FED-FEDO-201021/941
Out-of-bounds Write	08-Oct-21	6.8	Out of bounds write in V8 in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30632**	https://crbug.com/1247763 , https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	O-FED-FEDO-201021/942
Use After Free	08-Oct-21	6.8	Use after free in Indexed DB API in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a	https://crbug.com/1247766 , https://chromereleases.googleblog.com/2021/09/stable-channel-	O-FED-FEDO-201021/943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted HTML page. **CVE ID : CVE-2021-30633**	update-for-desktop.html	
Out-of-bounds Write	04-Oct-21	6.5	Redis is an open source, in-memory database that persists on disk. In affected versions specially crafted Lua scripts executing in Redis can cause the heap-based Lua stack to be overflowed, due to incomplete checks for this condition. This can result with heap corruption and potentially remote code execution. This problem exists in all versions of Redis with Lua scripting support, starting from 2.6. The problem is fixed in versions 6.2.6, 6.0.16 and 5.0.14. For users unable to update an additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from executing Lua scripts. This can be done using ACL to restrict EVAL and EVALSHA commands. **CVE ID : CVE-2021-32626**	https://github.com/redis/redis/commit/666ed7facf4524bf6d19b11b20faa2cf93fdf591, https://github.com/redis/redis/security/advisories/GHSA-p486-xggp-782c	O-FED-FEDO-201021/944
Integer Overflow or Wraparound	04-Oct-21	6	Redis is an open source, in-memory database that persists on disk. In affected versions an integer overflow bug in Redis can be exploited to corrupt the heap and potentially result with remote code execution. The	https://github.com/redis/redis/commit/f6a40570fa63d5afdd596c78083d754081d80ae3, https://github.com/redis/r	O-FED-FEDO-201021/945

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
			vulnerability involves changing the default proto-max-bulk-len and client-query-buffer-limit configuration parameters to very large values and constructing specially crafted very large stream elements. The problem is fixed in Redis 6.2.6, 6.0.16 and 5.0.14. For users unable to upgrade an additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the proto-max-bulk-len configuration parameter. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command. **CVE ID : CVE-2021-32627**	edis/security/advisories/GHSA-f434-69fm-g45v	
Integer Overflow or Wraparound	04-Oct-21	6	Redis is an open source, in-memory database that persists on disk. An integer overflow bug in the ziplist data structure used by all versions of Redis can be exploited to corrupt the heap and potentially result with remote code execution. The vulnerability involves modifying the default ziplist configuration parameters (hash-max-ziplist-entries, hash-max-	https://github.com/redis/redis/commit/f6a40570fa63d5afdd596c78083d754081d80ae3, https://github.com/redis/redis/security/advisories/GHSA-vw22-qm3h-49pr	O-FED-FEDO-201021/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ziplist-value, zset-max-ziplist-entries or zset-max-ziplist-value) to a very large value, and then constructing specially crafted commands to create very large ziplists. The problem is fixed in Redis versions 6.2.6, 6.0.16, 5.0.14. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the above configuration parameters. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command. **CVE ID : CVE-2021-32628**		
Allocation of Resources Without Limits or Throttling	04-Oct-21	5	Redis is an open source, in-memory database that persists on disk. When parsing an incoming Redis Standard Protocol (RESP) request, Redis allocates memory according to user-specified values which determine the number of elements (in the multi-bulk header) and size of each element (in the bulk header). An attacker delivering specially crafted requests over multiple connections can cause the server to allocate significant amount of memory. Because the same	https://github.com/redis/redis/commit/5674b0057ff2903d43eaff802017eddf37c360f8, https://github.com/redis/redis/security/advisories/GHSA-f6pw-v9gw-v64p	O-FED-FEDO-201021/947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing mechanism is used to handle authentication requests, this vulnerability can also be exploited by unauthenticated users. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. An additional workaround to mitigate this problem without patching the redis-server executable is to block access to prevent unauthenticated users from connecting to Redis. This can be done in different ways: Using network access control tools like firewalls, iptables, security groups, etc. or Enabling TLS and requiring users to authenticate using client side certificates. **CVE ID : CVE-2021-32675**		
Integer Overflow or Wraparound	04-Oct-21	6	Redis is an open source, in-memory database that persists on disk. An integer overflow bug affecting all versions of Redis can be exploited to corrupt the heap and potentially be used to leak arbitrary contents of the heap or trigger remote code execution. The vulnerability involves changing the default set-max-intset-entries configuration parameter to a very large value and	https://github.com/redis/redis/security/advisories/GHSA-m3mf-8x9w-r27q, https://github.com/redis/redis/commit/a30d367a71b7017581cf1ca104242a3c644dec0f	O-FED-FEDO-201021/948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			constructing specially crafted commands to manipulate sets. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the set-max-intset-entries configuration parameter. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command. **CVE ID : CVE-2021-32687**		
Integer Overflow or Wraparound	04-Oct-21	9	Redis is an open source, in-memory database that persists on disk. The redis-cli command line tool and redis-sentinel service may be vulnerable to integer overflow when parsing specially crafted large multi-bulk network replies. This is a result of a vulnerability in the underlying hiredis library which does not perform an overflow check before calling the calloc() heap allocation function. This issue only impacts systems with heap allocators that do not perform their own overflow checks. Most modern systems do and are therefore not likely to be	https://github.com/redis/redis/security/advisories/GHSA-833w-8v3m-8wwr, https://github.com/redis/redis/commit/0215324a66af949be39b34be2d55143232c1cb71	O-FED-FEDO-201021/949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected. Furthermore, by default redis-sentinel uses the jemalloc allocator which is also not vulnerable. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. **CVE ID : CVE-2021-32762**		
Google					
android					
Origin Validation Error	08-Oct-21	4.3	Inappropriate implementation in Compositing in Google Chrome on Android prior to 94.0.4606.54 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-37966**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1238944	O-GOO-ANDR-201021/950
Improper Privilege Management	06-Oct-21	4.6	In lockAllProfileTasks of RootWindowContainer.java , there is a possible way to access the work profile without the profile PIN, after logging in. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-177457096 **CVE ID : CVE-2021-0595**	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/951
Improper	06-Oct-21	4.4	In onCreate of	https://sourc	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			ConfirmConnectActivity.java, there is a possible pairing of untrusted Bluetooth devices due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-180422108 **CVE ID : CVE-2021-0598**	e.android.com/security/bulletin/2021-09-01	201021/952
N/A	06-Oct-21	6.8	When extracting the incorrectly formatted flv file, the memory is damaged, the playback interface shows that the video cannot be played, and the log is found to be crashed. This problem may lead to hacker malicious code attacks, resulting in the loss of user rights.Product: Androidversion:Android-10Android ID: A-189402477 **CVE ID : CVE-2021-0635**	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/953
N/A	06-Oct-21	6.8	When extracting the incorrectly formatted avi file, the memory is damaged, the playback interface shows that the video cannot be played, and the log is found to be crashed. This problem may	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to hacker malicious code attacks, resulting in the loss of user rights.Product: Androidversion: Android-10Android ID: A-189392423 **CVE ID : CVE-2021-0636**		
Incorrect Authorization	06-Oct-21	2.1	In conditionallyRemoveIdentifiers of SubscriptionController.java , there is a possible way to retrieve a trackable identifier due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-181053462 **CVE ID : CVE-2021-0644**	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/955
Incorrect Authorization	06-Oct-21	2.1	In system properties, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-192535676	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/956

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-2021-0680		
Incorrect Authorization	06-Oct-21	2.1	In system properties, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-192535337 **CVE ID : CVE-2021-0681**	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/957
Incorrect Authorization	06-Oct-21	2.1	In sendAccessibilityEvent of NotificationManagerService.java, there is a possible disclosure of notification data due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-159624555 **CVE ID : CVE-2021-0682**	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/958
N/A	06-Oct-21	4.6	In runTraceIpcStop of ActivityManagerShellCommand.java, there is a possible deletion of system files due to a confused	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-185398942 **CVE ID : CVE-2021-0683**		
Use After Free	06-Oct-21	4.6	In TouchInputMapper::sync of TouchInputMapper.cpp, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-179839665 **CVE ID : CVE-2021-0684**	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/960
Deserialization of Untrusted Data	06-Oct-21	4.6	In ParsedIntentInfo of ParsedIntentInfo.java, there is a possible parcel serialization/deserialization mismatch due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-11Android ID: A-191055353 **CVE ID : CVE-2021-0685**		
Incorrect Authorization	06-Oct-21	2.1	In getDefaultSmsPackage of RoleManagerService.java, there is a possible way to get information about the default sms app of a different device user due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-177927831 **CVE ID : CVE-2021-0686**	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/962
Improper Input Validation	06-Oct-21	1.9	In ellipsize of Layout.java, there is a possible ANR due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-188913943 **CVE ID : CVE-2021-0687**	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/963
Concurrent	06-Oct-21	4.4	In lockNow of	https://sourc	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
Execution using Shared Resource with Improper Synchronization ('Race Condition')			PhoneWindowManager.java, there is a possible lock screen bypass due to a race condition. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-161149543 **CVE ID : CVE-2021-0688**	e.android.com/security/bulletin/2021-09-01	201021/964
Out-of-bounds Read	06-Oct-21	2.1	In RGB_to_BGR1_portable of SkSwizzler_opts.h, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-190188264 **CVE ID : CVE-2021-0689**	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/965
Out-of-bounds Write	06-Oct-21	4.3	In ih264d_mark_err_slice_skip of ih264d_parse_pslice.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/966

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
			privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-182152757 **CVE ID : CVE-2021-0690**		
Improper Privilege Management	06-Oct-21	4.6	In the SELinux policy configured in system_app.te, there is a possible way for system_app to gain code execution in other processes due to an overly-permissive SELinux policy. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-188554048 **CVE ID : CVE-2021-0691**	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/967
Improper Privilege Management	06-Oct-21	4.6	In sendBroadcastToInstaller of FirstScreenBroadcast.java, there is a possible activity launch due to an unsafe PendingIntent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/968

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
			11 Android-9 Android-10Android ID: A-179289753 **CVE ID : CVE-2021-0692**		
N/A	06-Oct-21	2.1	In openFile of HeapDumpProvider.java, there is a possible way to retrieve generated heap dumps from debuggable apps due to an unprotected provider. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-184046948 **CVE ID : CVE-2021-0693**	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/969
Use After Free	06-Oct-21	2.1	In get_sock_stat of xt_qtaguid.c, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-184018316References: Upstream kernel **CVE ID : CVE-2021-0695**	https://source.android.com/security/bulletin/2021-09-01	O-GOO-ANDR-201021/970
Buffer Copy without Checking	06-Oct-21	7.2	Assuming system privilege is gained, possible buffer overflow vulnerabilities in	https://security.samsungmobile.com/sec	O-GOO-ANDR-201021/971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			the Vision DSP kernel driver prior to SMR Oct-2021 Release 1 allows privilege escalation to Root by hijacking loaded library. **CVE ID : CVE-2021-25467**	urityUpdate.smsb?year=2021&month=10	
Improper Input Validation	06-Oct-21	2.1	A possible guessing and confirming a byte memory vulnerability in Widevine trustlet prior to SMR Oct-2021 Release 1 allows attackers to read arbitrary memory address. **CVE ID : CVE-2021-25468**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/972
Out-of-bounds Write	06-Oct-21	4.6	A possible stack-based buffer overflow vulnerability in Widevine trustlet prior to SMR Oct-2021 Release 1 allows arbitrary code execution. **CVE ID : CVE-2021-25469**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/973
Incorrect Authorization	06-Oct-21	3.6	An improper caller check logic of SMC call in TEEGRIS secure OS prior to SMR Oct-2021 Release 1 can be used to compromise TEE. **CVE ID : CVE-2021-25470**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/974
N/A	06-Oct-21	5	A lack of replay attack protection in Security Mode Command process prior to SMR Oct-2021 Release 1 can lead to denial of service on mobile network connection and battery depletion. **CVE ID : CVE-2021-25471**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/975
Incorrect	06-Oct-21	2.1	An improper access control	https://securi	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			vulnerability in BluetoothSettingsProvider prior to SMR Oct-2021 Release 1 allows untrusted application to overwrite some Bluetooth information. **CVE ID : CVE-2021-25472**	ty.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	201021/976
Improper Handling of Exceptional Conditions	06-Oct-21	4.9	Assuming a shell privilege is gained, an improper exception handling for multi_sim_bar_hide_by_meadia_full value in SystemUI prior to SMR Oct-2021 Release 1 allows an attacker to cause a permanent denial of service in user device before factory reset. **CVE ID : CVE-2021-25473**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/977
Improper Handling of Exceptional Conditions	06-Oct-21	4.9	Assuming a shell privilege is gained, an improper exception handling for multi_sim_bar_show_on_qspanel value in SystemUI prior to SMR Oct-2021 Release 1 allows an attacker to cause a permanent denial of service in user device before factory reset. **CVE ID : CVE-2021-25474**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/978
Out-of-bounds Write	06-Oct-21	7.2	A possible heap-based buffer overflow vulnerability in DSP kernel driver prior to SMR Oct-2021 Release 1 allows arbitrary memory write and code execution.	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25475		
Incorrect Authorization	06-Oct-21	2.1	An information disclosure vulnerability in Widevine TA log prior to SMR Oct-2021 Release 1 allows attackers to bypass the ASLR protection mechanism in TEE. **CVE ID : CVE-2021-25476**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/980
Double Free	06-Oct-21	4	An improper error handling in Mediatek RRC Protocol stack prior to SMR Oct-2021 Release 1 allows modem crash and remote denial of service. **CVE ID : CVE-2021-25477**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/981
Out-of-bounds Write	06-Oct-21	6.5	A possible stack-based buffer overflow vulnerability in Exynos CP Chipset prior to SMR Oct-2021 Release 1 allows arbitrary memory write and code execution. **CVE ID : CVE-2021-25478**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/982
Out-of-bounds Write	06-Oct-21	6.5	A possible heap-based buffer overflow vulnerability in Exynos CP Chipset prior to SMR Oct-2021 Release 1 allows arbitrary memory write and code execution. **CVE ID : CVE-2021-25479**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/983
Authentication Bypass by Capture-replay	06-Oct-21	5	A lack of replay attack protection in GUTI REALLOCATION COMMAND message process in Qualcomm modem prior to SMR Oct-	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=1	O-GOO-ANDR-201021/984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021 Release 1 can lead to remote denial of service on mobile network connection. **CVE ID : CVE-2021-25480**	0	
Improper Check for Unusual or Exceptional Conditions	06-Oct-21	4.6	An improper error handling in Exynos CP booting driver prior to SMR Oct-2021 Release 1 allows local attackers to bypass a Secure Memory Protector of Exynos CP Memory. **CVE ID : CVE-2021-25481**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/985
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-21	3.6	SQL injection vulnerabilities in CMFA framework prior to SMR Oct-2021 Release 1 allow untrusted application to overwrite some CMFA framework information. **CVE ID : CVE-2021-25482**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/986
Out-of-bounds Read	06-Oct-21	5	Lack of boundary checking of a buffer in livfivextractor library prior to SMR Oct-2021 Release 1 allows OOB read. **CVE ID : CVE-2021-25483**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/987
Improper Authentication	06-Oct-21	2.1	Improper authentication in InputManagerService prior to SMR Oct-2021 Release 1 allows monitoring the touch event. **CVE ID : CVE-2021-25484**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/988
Improper Limitation of a Pathname	06-Oct-21	5.8	Path traversal vulnerability in FactoryAirCommnadMange	https://security.samsungmobile.com/sec	O-GOO-ANDR-201021/989

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
to a Restricted Directory ('Path Traversal')			r prior to SMR Oct-2021 Release 1 allows attackers to write file as system UID via BT remote socket. **CVE ID : CVE-2021-25485**	urityUpdate.smsb?year=2021&month=10	
N/A	06-Oct-21	2.1	Exposure of information vulnerability in ipcdump prior to SMR Oct-2021 Release 1 allows an attacker detect device information via analyzing packet in log. **CVE ID : CVE-2021-25486**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/990
Out-of-bounds Read	06-Oct-21	4.6	Lack of boundary checking of a buffer in set_skb_priv() of modem interface driver prior to SMR Oct-2021 Release 1 allows OOB read and it results in arbitrary code execution by dereference of invalid function pointer. **CVE ID : CVE-2021-25487**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/991
Out-of-bounds Read	06-Oct-21	2.1	Lack of boundary checking of a buffer in recv_data() of modem interface driver prior to SMR Oct-2021 Release 1 allows OOB read. **CVE ID : CVE-2021-25488**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/992
Improper Input Validation	06-Oct-21	4.9	Assuming radio permission is gained, missing input validation in modem interface driver prior to SMR Oct-2021 Release 1 results in format string bug leading to kernel panic. **CVE ID : CVE-2021-25489**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Oct-21	3.6	A keyblob downgrade attack in keymaster prior to SMR Oct-2021 Release 1 allows attacker to trigger IV reuse vulnerability with privileged process. **CVE ID : CVE-2021-25490**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/994
NULL Pointer Dereference	06-Oct-21	2.1	A vulnerability in mfc driver prior to SMR Oct-2021 Release 1 allows memory corruption via NULL-pointer dereference. **CVE ID : CVE-2021-25491**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10	O-GOO-ANDR-201021/995
chrome_os					
N/A	08-Oct-21	4.3	Inappropriate implementation in ChromeOS Networking in Google Chrome on ChromeOS prior to 94.0.4606.54 allowed an attacker with a rogue wireless access point to to potentially carryout a wifi impersonation attack via a crafted ONC file. **CVE ID : CVE-2021-37964**	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html, https://crbug.com/1203612	O-GOO-CHRO-201021/996
IBM					
aix					
Generation of Error Message Containing Sensitive Information	07-Oct-21	4	IBM Sterling File Gateway 6.0.0.0 through 6.1.1.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further	https://www.ibm.com/support/pages/node/6496771, https://exchange.xforce.ibmcloud.com/vulnerabilities/199170	O-IBM-AIX-201021/997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks against the system. IBM X-Force ID: 199170. **CVE ID : CVE-2021-20552**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-21	7.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.1.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 203734. **CVE ID : CVE-2021-29798**	https://www.ibm.com/support/pages/node/6495925, https://exchange.xforce.ibmcloud.com/vulnerabilities/203734	O-IBM-AIX-201021/998
powervm_hypervisor_firmware					
N/A	06-Oct-21	6.5	IBM PowerVM Hypervisor FW1010 could allow a privileged user to gain access to another VM due to assigning duplicate WWPNs. IBM X-Force ID: 210162. **CVE ID : CVE-2021-38923**	https://exchange.xforce.ibmcloud.com/vulnerabilities/210162, https://www.ibm.com/support/pages/node/6495879	O-IBM-POWE-201021/999
ts7700_firmware					
Improper Authentication	06-Oct-21	10	The IBM TS7700 Management Interface is vulnerable to unauthenticated access. By accessing a specially-crafted URL, an attacker may gain administrative access to the Management Interface without authentication. IBM X-Force ID: 207747.	https://www.ibm.com/support/pages/node/6495469, https://exchange.xforce.ibmcloud.com/vulnerabilities/207747	O-IBM-TS77-201021/1000

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
		🟥	**CVE ID : CVE-2021-29908**		
Insyde					
insydeh2o					
Inclusion of Functionality from Untrusted Control Sphere	01-Oct-21	4.6	In the kernel in Insyde InsydeH2O 5.x, certain SMM drivers did not correctly validate the CommBuffer and CommBufferSize parameters, allowing callers to corrupt either the firmware or the OS memory. The fixed versions for this issue in the PnpSmm, SmmResourceCheckDxe, and BeepStatusCode drivers are 05.08.23, 05.16.23, 05.26.23, 05.35.23, 05.43.23, and 05.51.23 (for Kernel 5.0 through 5.5). **CVE ID : CVE-2021-33626**	https://www.insyde.com/security-pledge/SA-2021001	O-INS-INSY-201021/1001
lancom-systems					
lcos					
N/A	07-Oct-21	8.5	In LCOS 10.40 to 10.42.0473-RU3 with SNMPv3 enabled on LANCOM devices, changing the password of the root user via the CLI does not change the password of the root user for SNMPv3 access. (However, changing the password of the root user via LANconfig does change the password of the root user for SNMPv3	N/A	O-LAN-LCOS-201021/1002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access.) **CVE ID : CVE-2021-33903**		
Linux					
linux_kernel					
Integer Overflow or Wraparound	02-Oct-21	4.6	prealloc_elems_and_freelist in kernel/bpf/stackmap.c in the Linux kernel through 5.14.9 allows unprivileged users to trigger an eBPF multiplication integer overflow with a resultant out-of-bounds write. **CVE ID : CVE-2021-41864**	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf.git/commit/?id=30e29a9a2bc6a4888335a6ede968b75cd329657a, https://github.com/torvalds/linux/commit/30e29a9a2bc6a4888335a6ede968b75cd329657a	O-LIN-LINU-201021/1003
Out-of-bounds Write	05-Oct-21	6.9	The decode_data function in drivers/net/hamradio/6pack.c in the Linux kernel before 5.13.13 has a slab out-of-bounds write. Input from a process that has the CAP_NET_ADMIN capability can lead to root access. **CVE ID : CVE-2021-42008**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=19d1532a187669ce86d5a2696eb7275310070793, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.13	O-LIN-LINU-201021/1004
Generation of Error Message	07-Oct-21	4	IBM Sterling File Gateway 6.0.0.0 through 6.1.1.0 could allow a remote	https://www.ibm.com/support/pages/n	O-LIN-LINU-201021/1005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Containing Sensitive Information			attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 199170. **CVE ID : CVE-2021-20552**	ode/6496771, https://exchange.xforce.ibmcloud.com/vulnerabilities/199170	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-21	7.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.1.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 203734. **CVE ID : CVE-2021-29798**	https://www.ibm.com/support/pages/node/6495925, https://exchange.xforce.ibmcloud.com/vulnerabilities/203734	O-LIN-LINU-201021/1006
Time-of-check Time-of-use (TOCTOU) Race Condition	06-Oct-21	6.9	A vulnerability in the shared library loading mechanism of Cisco AnyConnect Secure Mobility Client for Linux and Mac OS could allow an authenticated, local attacker to perform a shared library hijacking attack on an affected device if the VPN Posture (HostScan) Module is installed on the AnyConnect client. This vulnerability is due to a race condition in the signature verification process for shared library	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-lib-hija-cAFB7x4q	O-LIN-LINU-201021/1007

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
			files that are loaded on an affected device. An attacker could exploit this vulnerability by sending a series of crafted interprocess communication (IPC) messages to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected device with root privileges. To exploit this vulnerability, the attacker must have a valid account on the system. **CVE ID : CVE-2021-34788**		
Microsoft					
windows					
Improper Privilege Management	01-Oct-21	4.6	The Windows version of Multipass before 1.7.0 allowed any local process to connect to the localhost TCP control socket to perform mounts from the operating system to a guest, allowing for privilege escalation. **CVE ID : CVE-2021-3626**	https://github.com/canonical/multipass/pull/2150	O-MIC-WIND-201021/1008
Improper Privilege Management	06-Oct-21	2.1	An arbitrary file creation by privilege escalation vulnerability in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1, and Worry-Free Business Security Services could allow a local attacker to	https://success.trendmicro.com/solution/000289183	O-MIC-WIND-201021/1009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			create an arbitrary file with higher privileges that could lead to a denial-of-service (DoS) on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-3848**		
Unquoted Search Path or Element	04-Oct-21	4.4	In Akamai EAA (Enterprise Application Access) Client before 2.3.1, 2.4.x before 2.4.1, and 2.5.x before 2.5.3, an unquoted path may allow an attacker to hijack the flow of execution. **CVE ID : CVE-2021-40683**	https://www.akamai.com/products/enterprise-application-access, https://akamai.com/blog/news/eaa-client-escalation-of-privilege-vulnerability	O-MIC-WIND-201021/1010
Use After Free	07-Oct-21	6.8	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability when processing AcroForm listbox that could result in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability in that the target must visit a	https://helpx.adobe.com/security/products/acrobat/apsb21-55.html	O-MIC-WIND-201021/1011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious page or open a malicious file. **CVE ID : CVE-2021-40725**		
Use After Free	07-Oct-21	6.8	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a use-after-free vulnerability when processing AcroForm field that could result in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **CVE ID : CVE-2021-40726**	https://helpx.adobe.com/security/products/acrobat/apsb21-55.html	O-MIC-WIND-201021/1012
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVRDL unpacking module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-40832**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-40832	O-MIC-WIND-201021/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	07-Oct-21	4	IBM Sterling File Gateway 6.0.0.0 through 6.1.1.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 199170. **CVE ID : CVE-2021-20552**	https://www.ibm.com/support/pages/node/6496771, https://exchange.xforce.ibmcloud.com/vulnerabilities/199170	O-MIC-WIND-201021/1014
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Oct-21	4.3	In PHP versions 7.3.x below 7.3.31, 7.4.x below 7.4.24 and 8.0.x below 8.0.11, in Microsoft Windows environment, ZipArchive::extractTo may be tricked into writing a file outside target directory when extracting a ZIP file, thus potentially causing files to be created or overwritten, subject to OS permissions. **CVE ID : CVE-2021-21706**	https://bugs.php.net/bug.php?id=81420	O-MIC-WIND-201021/1015
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-21	7.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.1.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 203734. **CVE ID : CVE-2021-29798**	https://www.ibm.com/support/pages/node/6495925, https://exchange.xforce.ibmcloud.com/vulnerabilities/203734	O-MIC-WIND-201021/1016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Oct-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the AVPACK module component used in certain F-Secure products can crash while scanning a fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33603**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-33603	O-MIC-WIND-201021/1017
Mitsubishielectric					
got2000_gt2103-pmbd_firmware					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	O-MIT-GOT2-201021/1018

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
			specially crafted packets. **CVE ID : CVE-2021-20602**		
got2000_gt2104-pmbd_firmware					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	O-MIT-GOT2-201021/1019
got2000_gt2104-rtbd_firmware					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	O-MIT-GOT2-201021/1020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**		
got2000_gt2107-wtbd_firmware					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	O-MIT-GOT2-201021/1021
got2000_gt2107-wtsd_firmware					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	O-MIT-GOT2-201021/1022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**		
got_simple_gs2107-wtbd-n_firmware					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	O-MIT-GOT_-201021/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
got_simple_gs2107-wtbd_firmware					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	O-MIT-GOT_-201021/1024
got_simple_gs2110-wtbd-n_firmware					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	O-MIT-GOT_-201021/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**		
got_simple_gs2110-wtbd_firmware					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	O-MIT-GOT_-201021/1026
le7-40gu-l_firmware					
Improper Handling of Exceptional Conditions	07-Oct-21	5	Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf	O-MIT-LE7--201021/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets. **CVE ID : CVE-2021-20602**		
r12ccpu-v_firmware					
Uncontrolled Resource Consumption	08-Oct-21	4.3	Uncontrolled resource consumption in MELSEC iQ-R series C Controller Module R12CCPU-V all versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending a large number of packets in a short time while the module starting up. **CVE ID : CVE-2021-20600**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-015_en.pdf	O-MIT-R12C-201021/1028
Polycom					
vvx_400_firmware					
Improper Privilege Management	04-Oct-21	6.5	Polycom VVX 400/410 version 5.3.1 allows low-privileged users to change the Admin account password by modifying a POST parameter name during the password reset process. **CVE ID : CVE-2021-41322**	https://support.polycom.com/content/support.html	O-POL-VVX_-201021/1029
vvx_410_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	04-Oct-21	6.5	Polycom VVX 400/410 version 5.3.1 allows low-privileged users to change the Admin account password by modifying a POST parameter name during the password reset process. **CVE ID : CVE-2021-41322**	https://support.polycom.com/content/support.html	O-POL-VVX_-201021/1030
ptcl					
hg150-ub_firmware					
Improper Authentication	04-Oct-21	7.5	An issue in the administrator authentication panel of PTCL HG150-Ub v3.0 allows attackers to bypass authentication via modification of the cookie value and Response Path. **CVE ID : CVE-2021-35296**	N/A	O-PTC-HG15-201021/1031
Redhat					
enterprise_linux					
Out-of-bounds Read	04-Oct-21	4	Redis is an open source, in-memory database that persists on disk. When using the Redis Lua Debugger, users can send malformed requests that cause the debugger's protocol parser to read data beyond the actual buffer. This issue affects all versions of Redis with Lua debugging support (3.2 or newer). The problem is fixed in versions 6.2.6, 6.0.16 and 5.0.14. **CVE ID : CVE-2021-32672**	https://github.com/redis/redis/security/advisories/GHSA-9mj9-xx53-qmxm, https://github.com/redis/redis/commit/6ac3c0b7abd35f37201ed2d6298ecef4ea1ae1dd	O-RED-ENTE-201021/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
visual-tools					
dvr_vx16_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Oct-21	10	In Visual Tools DVR VX16 4.2.28.0, an unauthenticated attacker can achieve remote command execution via shell metacharacters in the cgi-bin/slogin/login.py User-Agent HTTP header. **CVE ID : CVE-2021-42071**	https://visual-tools.com/	O-VIS-DVR_-201021/1033
XEN					
xen					
Improper Privilege Management	06-Oct-21	4.6	PCI devices with RMRRs not deassigned correctly Certain PCI devices in a system might be assigned Reserved Memory Regions (specified via Reserved Memory Region Reporting, "RMRR"). These are typically used for platform tasks such as legacy USB emulation. If such a device is passed through to a guest, then on guest shutdown the device is not properly deassigned. The IOMMU configuration for these devices which are not properly deassigned ends up pointing to a freed data structure, including the IO Pagetables. Subsequent DMA or interrupts from the device will have unpredictable behaviour, ranging from IOMMU faults to memory corruption.	https://xenbits.xenproject.org/xsa/advisory-386.txt	O-XEN-XEN-201021/1034

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-2021-28702		
zephyrproject					
zephyr					
Out-of-bounds Write	05-Oct-21	7.5	Buffer overflow in Zephyr USB DFU DNLOAD. Zephyr versions >= v2.5.0 contain Heap-based Buffer Overflow (CWE-122). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-c3gr-hgvr-f363 **CVE ID : CVE-2021-3625**	N/A	O-ZEP-ZEPH-201021/1035
NULL Pointer Dereference	05-Oct-21	7.5	DOS: Incorrect 802154 Frame Validation for Omitted Source / Dest Addresses. Zephyr versions >= > v2.4.0 contain NULL Pointer Dereference (CWE-476), Attempt to Access Child of a Non-structure Pointer (CWE-588). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-94jg-2p6q-5364 **CVE ID : CVE-2021-3319**	http://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-94jg-2p6q-5364	O-ZEP-ZEPH-201021/1036
N/A	05-Oct-21	6.4	BT: Possible to overwrite an existing bond during keys distribution phase when the identity address of the bond is known. Zephyr versions >= 1.14.2, >= 2.4.0, >= 2.5.0 contain Use of Multiple Resources	http://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-j76f-35mc-	O-ZEP-ZEPH-201021/1037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with Duplicate Identifier (CWE-694). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-j76f-35mc-4h63 **CVE ID : CVE-2021-3436**	4h63	
N/A	05-Oct-21	5	Zephyr JSON decoder incorrectly decodes array of array. Zephyr versions >= >1.14.0, >= >2.5.0 contain Attempt to Access Child of a Non-structure Pointer (CWE-588). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-289f-7mw3-2qf4 **CVE ID : CVE-2021-3510**	http://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-289f-7mw3-2qf4	O-ZEP-ZEPH-201021/1038
N/A	05-Oct-21	5.8	Buffer Access with Incorrect Length Value in zephyr. Zephyr versions >= >=2.5.0 contain Buffer Access with Incorrect Length Value (CWE-805). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-8q65-5gqf-fmw5 **CVE ID : CVE-2021-3581**	N/A	O-ZEP-ZEPH-201021/1039