Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
10web					
photo_gallery					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	The Photo Gallery by 10Web - Mobile-Friendly Image Gallery WordPress plugin before 1.5.67 did not properly sanitise the gallery title, allowing high privilege users to create one with XSS payload in it, which will be triggered when another user will view the gallery list or the affected gallery in the admin dashboard. This is due to an incomplete fix of CVE-2019-16117 **CVE ID : CVE-2021-24310**	https://wpscan.com/vulnerability/f34096ec-b1b0-471d-88a4-4699178a3165	A-10W-PHOT-180621/1
2ndquadrant					
pglogical					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Jun-21	7.2	A shell injection flaw was found in pglogical in versions before 2.3.4 and before 3.6.26. An attacker with CREATEDB privileges on a PostgreSQL server can craft a database name that allows execution of shell commands as the postgresql user when calling pglogical.create_subscription( ). **CVE ID : CVE-2021-3515**	https://bugzilla.redhat.com/show_bug.cgi?id=1954112	A-2ND-PGLO-180621/2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Accela					
civic_platform					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-21	4.3	In Accela Civic Platform through 21.1, the security/hostSignon.do parameter servProvCode is vulnerable to XSS. **CVE ID : CVE-2021-33904**	N/A	A-ACC-CIVI-180621/3
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-21	4.3	Accela Civic Platform through 20.1 allows ssoAdapter/logoutAction.do successURL XSS. **CVE ID : CVE-2021-34370**	N/A	A-ACC-CIVI-180621/4
Adiscon					
loganalyzer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-21	4.3	Adiscon LogAnalyzer 4.1.10 and 4.1.11 allow login.php XSS. **CVE ID : CVE-2021-31738**	N/A	A-ADI-LOGA-180621/5
aomedia					
aomedia					
Use After Free	02-Jun-21	7.5	aom_dsp/grain_table.c in libaom in AOMedia before 2021-03-30 has a use-after-free. **CVE ID : CVE-2021-30474**	https://aomedia.googlesource.com/aom/+/6e31957b6dc62dbc7d1bb70cd84902dd14c4bf2e	A-AOM-AOME-180621/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Jun-21	7.5	aom_dsp/noise_model.c in libaom in AOMedia before 2021-03-24 has a buffer overflow. **CVE ID : CVE-2021-30475**	https://aomedia.googlesource.com/aom/+/12adc723acf02633595a4d8da8345742729f46c0	A-AOM-AOME-180621/7
Apache					
dubbo					
Deserialization of Untrusted Data	01-Jun-21	7.5	Apache Dubbo prior to 2.6.9 and 2.7.9 by default supports generic calls to arbitrary methods exposed by provider interfaces. These invocations are handled by the GenericFilter which will find the service and method specified in the first arguments of the invocation and use the Java Reflection API to make the final call. The signature for the $invoke or $invokeAsync methods is Ljava/lang/String;[Ljava/lang/String;[Ljava/lang/Object; where the first argument is the name of the method to invoke, the second one is an array with the parameter types for the method being invoked and the third one is an array with the actual call arguments. In addition, the caller also needs to set an RPC attachment specifying that the call is a generic call and how to decode the arguments. The possible values are: - true - raw.return	https://lists.apache.org/thread.html/rccbcbdd6593e42ea3a1e8fedd12807cb111375c9c40edb005ef36f67@%3Cdev.dubbo.apache.org%3E, https://lists.apache.org/thread.html/rccbcbdd6593e42ea3a1e8fedd12807cb111375c9c40edb005ef36f67%40%3Cdev.dubbo.apache.org%3E	A-APA-DUBB-180621/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			- nativejava - bean - protobuf-json An attacker can control this RPC attachment and set it to nativejava to force the java deserialization of the byte array located in the third argument. **CVE ID : CVE-2021-30179**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	01-Jun-21	6.8	Apache Dubbo prior to 2.7.9 support Tag routing which will enable a customer to route the request to the right server. These rules are used by the customers when making a request in order to find the right endpoint. When parsing these YAML rules, Dubbo customers may enable calling arbitrary constructors. **CVE ID : CVE-2021-30180**	https://lists.apache.org/thread.html/raed526465e56204030ddf374b1959478a290e7511971d7aba2e9e39b%40%3Cdev.dubbo.apache.org%3E	A-APA-DUBB-180621/9
N/A	01-Jun-21	7.5	Apache Dubbo prior to 2.6.9 and 2.7.9 supports Script routing which will enable a customer to route the request to the right server. These rules are used by the customers when making a request in order to find the right endpoint. When parsing these rules, Dubbo customers use ScriptEngine and run the rule provided by the script which by default may enable executing arbitrary code. **CVE ID : CVE-2021-30181**	https://lists.apache.org/thread.html/re22410dc704a09bc7032ddf15140cf5e7df3e8ece390fc9032ff5587%40%3Cdev.dubbo.apache.org%3E	A-APA-DUBB-180621/10
Server-Side Request Forgery (SSRF)	01-Jun-21	5.8	In Apache Dubbo prior to 2.6.9 and 2.7.9, the usage of parseURL method will lead to the bypass of white host	https://lists.apache.org/thread.html/re4cab88553	A-APA-DUBB-180621/11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check which can cause open redirect or SSRF vulnerability. **CVE ID : CVE-2021-25640**	61a454d2af106fb3dad76259e723015fd7e09cb4f9eb77%40%3Cdev.dubbo.apache.org%3E, https://lists.apache.org/thread.html/re4cab8855361a454d2af106fb3dad76259e723015fd7e09cb4f9eb77@%3Cdev.dubbo.apache.org%3E	
Deserialization of Untrusted Data	01-Jun-21	7.5	Each Apache Dubbo server will set a serialization id to tell the clients which serialization protocol it is working on. But for Dubbo versions before 2.7.8 or 2.6.9, an attacker can choose which serialization id the Provider will use by tampering with the byte preamble flags, aka, not following the server's instruction. This means that if a weak deserializer such as the Kryo and FST are somehow in code scope (e.g. if Kryo is somehow a part of a dependency), a remote unauthenticated attacker can tell the Provider to use the weak deserializer, and then proceed to exploit it.	https://lists.apache.org/thread.html/r99ef7fa35585d3a68762de07e8d2b2bc48b8fa669a03e8d84b9673f3%40%3Cdev.dubbo.apache.org%3E	A-APA-DUBB-180621/12

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25641		
Atlassian					
data_center					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-21	4.3	The number range searcher component in Jira Server and Jira Data Center before version 8.5.14, from version 8.6.0 before version 8.13.6, and from version 8.14.0 before version 8.16.1 allows remote attackers inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability. **CVE ID : CVE-2021-26078**	https://jira.atlassian.com/browse/JRASERVER-72392	A-ATL-DATA-180621/13
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-21	4.3	EditworkflowScheme.jspa in Jira Server and Jira Data Center before version 8.5.14, and from version 8.6.0 before version 8.13.6, and from 8.14.0 before 8.16.1 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability. **CVE ID : CVE-2021-26080**	https://jira.atlassian.com/browse/JRASERVER-72432	A-ATL-DATA-180621/14
jira					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-21	4.3	The number range searcher component in Jira Server and Jira Data Center before version 8.5.14, from version 8.6.0 before version 8.13.6, and from version 8.14.0 before version 8.16.1 allows remote attackers inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability.	https://jira.atlassian.com/browse/JRASERVER-72392	A-ATL-JIRA-180621/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26078		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-21	4.3	EditworkflowScheme.jspa in Jira Server and Jira Data Center before version 8.5.14, and from version 8.6.0 before version 8.13.6, and from 8.14.0 before 8.16.1 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability. **CVE ID : CVE-2021-26080**	https://jira.atlassian.com/browse/JRASERVER-72432	A-ATL-JIRA-180621/16
Automattic					
wp_super_cache					
Improper Control of Generation of Code ('Code Injection')	01-Jun-21	6.5	The parameters $cache_path, $wp_cache_debug_ip, $wp_super_cache_front_page_text, $cache_scheduled_time, $cached_direct_pages used in the settings of WP Super Cache WordPress plugin before 1.7.3 result in RCE because they allow input of '$' and '\n'. This is due to an incomplete fix of CVE-2021-24209. **CVE ID : CVE-2021-24312**	https://wpscan.com/vulnerability/2142c3d3-9a7f-4e3c-8776-d469a355d62f	A-AUT-WP_S-180621/17
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	The WP Super Cache WordPress plugin before 1.7.3 did not properly sanitise its wp_cache_location parameter in its settings, which could lead to a Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24329**	https://wpscan.com/vulnerability/9df86d05-1408-4c22-af55-5e3d44249fd0	A-AUT-WP_S-180621/18
Avahi					
avahi					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jun-21	2.1	A flaw was found in avahi in versions 0.6 up to 0.8. The event used to signal the termination of the client connection on the avahi Unix socket is not correctly handled in the client_work function, allowing a local attacker to trigger an infinite loop. The highest threat from this vulnerability is to the availability of the avahi service, which becomes unresponsive after this flaw is triggered. **CVE ID : CVE-2021-3468**	N/A	A-AVA-AVAH-180621/19
backstage					
backstage					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Jun-21	3.5	Backstage is an open platform for building developer portals, and techdocs-common contains common functionalities for Backstage's TechDocs. In `@backstage/techdocs-common` versions prior to 0.6.3, a malicious actor could read sensitive files from the environment where TechDocs documentation is built and published by setting a particular path for `docs_dir` in `mkdocs.yml`. These files would then be available over the TechDocs backend API. This vulnerability is mitigated by the fact that an attacker would need access to modify the `mkdocs.yml` in the	https://github.com/backstage/backstage/commit/8cefadca04cbf01d0394b0cb1983247e5f1d6208, https://github.com/backstage/backstage/security/advisories/GHSA-pgf8-28gg-vpr6	A-BAC-BACK-180621/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			documentation source code, and would also need access to the TechDocs backend API. The vulnerability is patched in the `0.6.3` release of `@backstage/techdocs-common`. **CVE ID : CVE-2021-32662**		
bdew					
bdlib					
Deserialization of Untrusted Data	03-Jun-21	7.5	The BDew BdLib library before 1.16.1.7 for Minecraft allows remote code execution because it deserializes untrusted data in ObjectInputStream.readObject as part of its use of Java serialization. **CVE ID : CVE-2021-33806**	https://bdew.net, https://github.com/bdew-minecraft/bdlib/commit/447210530ceec72fb3374efecb0930ed359d2297	A-BDE-BDLI-180621/21
boldthemes					
bello_-_directory_\\&_listing					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	The Bello - Directory & Listing WordPress theme before 1.6.0 did not properly sanitise its post_excerpt parameter before outputting it back in the shop/my-account/bello-listing-endpoint/ page, leading to a Cross-Site Scripting issue **CVE ID : CVE-2021-24319**	https://wpscan.com/vulnerability/2c274eb7-25f1-49d4-a2c8-8ce8cecebe68	A-BOL-BELL-180621/22
Improper Neutralization of Input During Web Page Generation	01-Jun-21	4.3	The Bello - Directory & Listing WordPress theme before 1.6.0 did not properly sanitise and escape its listing_list_view, bt_bb_listing_field_my_lat,	https://wpscan.com/vulnerability/6b5b42fd-028a-4405-b027-3266058029	A-BOL-BELL-180621/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			bt_bb_listing_field_my_lng, bt_bb_listing_field_distance_value, bt_bb_listing_field_my_lat_default, bt_bb_listing_field_keyword, bt_bb_listing_field_location_autocomplete, bt_bb_listing_field_price_range_from and bt_bb_listing_field_price_range_to parameter in ints listing page, leading to reflected Cross-Site Scripting issues. **CVE ID : CVE-2021-24320**	bb	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Jun-21	7.5	The Bello - Directory & Listing WordPress theme before 1.6.0 did not sanitise the bt_bb_listing_field_price_range_to, bt_bb_listing_field_now_open, bt_bb_listing_field_my_lng, listing_list_view and bt_bb_listing_field_my_lat parameters before using them in a SQL statement, leading to SQL Injection issues **CVE ID : CVE-2021-24321**	https://wpscan.com/vulnerability/7314f9fa-c047-4e0c-b145-940240a50c02	A-BOL-BELL-180621/24
bubble_fireworks_project					
bubble_fireworks					
Improper Verification of Cryptographic Signature	04-Jun-21	5	bubble fireworks is an open source java package relating to Spring Framework. In bubble fireworks before version 2021.BUILD-SNAPSHOT there is a vulnerability in which the	https://github.com/fxbin/bubble-fireworks/security/advisories/GHSA-hj36-84cp-	A-BUB-BUBB-180621/25

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			package did not properly verify the signature of JSON Web Tokens. This allows to forgery of valid JWTs. **CVE ID : CVE-2021-29500**	29pr	
cartflows					
funnel_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	The Funnel Builder by CartFlows â€“ Create High Converting Sales Funnels For WordPress plugin before 1.6.13 did not sanitise its facebook_pixel_id and google_analytics_id settings, allowing high privilege users to set XSS payload in them, which will either be executed on pages generated by the plugin, or the whole website depending on the settings used. **CVE ID : CVE-2021-24330**	https://wpscan.com/vulnerability/b9748066-83b7-4762-9124-de021f687477	A-CAR-FUNN-180621/26
Cisco					
common_services_platform_collector					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Jun-21	9	A vulnerability in the configuration dashboard of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to execute arbitrary code. This vulnerability is due to insufficient sanitization of configuration entries. An attacker could exploit this vulnerability by logging in as a super admin and entering crafted input to configuration options on the CSPC	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-CSPC-CIV-kDuBfNfu	A-CIS-COMM-180621/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration dashboard. A successful exploit could allow the attacker to execute remote code as root. **CVE ID : CVE-2021-1538**		
sd-wan_vbond_orchestrator					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	A-CIS-SD-W-180621/28
sd-wan_vmanage					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	A-CIS-SD-W-180621/29

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**		
thousandeyes_recorder					
Insufficiently Protected Credentials	04-Jun-21	2.1	A vulnerability in the installer software of Cisco ThousandEyes Recorder could allow an unauthenticated, local attacker to access sensitive information that is contained in the ThousandEyes Recorder installer software. This vulnerability exists because sensitive information is included in the application installer. An attacker could exploit this vulnerability by downloading the installer and extracting its contents. A successful exploit could allow the attacker to access sensitive information that is included in the application installer. **CVE ID : CVE-2021-1537**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-te-recorder-infodis-mx3ETTBM	A-CIS-THOU-180621/30
virtualized_packet_core					
Incorrect Authorization	04-Jun-21	6.5	Multiple vulnerabilities in the authorization process of Cisco ASR 5000 Series Software (StarOS) could allow an authenticated, remote attacker to bypass authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-autho-bypass-mJDF5S7n	A-CIS-VIRT-180621/31

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			section of this advisory. **CVE ID : CVE-2021-1539**		
Incorrect Authorization	04-Jun-21	6	Multiple vulnerabilities in the authorization process of Cisco ASR 5000 Series Software (StarOS) could allow an authenticated, remote attacker to bypass authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1540**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-autho-bypass-mJDF5S7n	A-CIS-VIRT-180621/32
vsmart_controller					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	A-CIS-VSMA-180621/33
webex_meetings					
Exposure of Sensitive System Information	04-Jun-21	2.1	A vulnerability in logging mechanisms of Cisco Webex Meetings client software could allow an authenticated,	https://tools.cisco.com/security/center/content/Cis	A-CIS-WEBE-180621/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to an Unauthorized Control Sphere			local attacker to gain access to sensitive information. This vulnerability is due to unsafe logging of application actions. An attacker could exploit this vulnerability by logging onto the local system and accessing files containing the logged details. A successful exploit could allow the attacker to gain access to sensitive information, including meeting data and recorded meeting transcriptions. **CVE ID : CVE-2021-1544**	coSecurityAdvisory/cisco-sa-webex-8fpBnKOz	
webex_meetings_desktop					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Jun-21	6.8	A vulnerability in Cisco Webex Network Recording Player for Windows and MacOS and Cisco Webex Player for Windows and MacOS could allow an attacker to execute arbitrary code on an affected system. The vulnerability is due to insufficient validation of values within Webex recording files formatted as either Advanced Recording Format (ARF) or Webex Recording Format (WRF). An attacker could exploit the vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file. A successful exploit could allow the attacker to execute	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-player-dOJ2jOJ	A-CIS-WEBE-180621/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on the affected system with the privileges of the targeted user. **CVE ID : CVE-2021-1502**		
Uncontrolled Search Path Element	04-Jun-21	6.9	A vulnerability in Cisco Webex Meetings Desktop App for Windows, Cisco Webex Meetings Server, Cisco Webex Network Recording Player for Windows, and Cisco Webex Teams for Windows could allow an authenticated, local attacker to perform a DLL injection attack on an affected device. To exploit this vulnerability, the attacker must have valid credentials on the Windows system. This vulnerability is due to incorrect handling of directory paths at run time. An attacker could exploit this vulnerability by inserting a configuration file in a specific path in the system, which can cause a malicious DLL file to be loaded when the application starts. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of another user account. **CVE ID : CVE-2021-1536**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-dll-inject-XNmcSGTU	A-CIS-WEBE-180621/36
webex_meetings_online					
Improper Restriction of Operations within the	04-Jun-21	6.8	A vulnerability in Cisco Webex Network Recording Player for Windows and MacOS and Cisco Webex Player for Windows and	https://tools.cisco.com/security/center/content/CiscoSecurityAd	A-CIS-WEBE-180621/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			MacOS could allow an attacker to execute arbitrary code on an affected system. The vulnerability is due to insufficient validation of values within Webex recording files formatted as either Advanced Recording Format (ARF) or Webex Recording Format (WRF). An attacker could exploit the vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user. **CVE ID : CVE-2021-1502**	visory/cisco-sa-webex-player-dOJ2jOJ	
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	A vulnerability in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to redirect users to a malicious file. This vulnerability is due to improper validation of URL paths in the application interface. An attacker could exploit this vulnerability by persuading a user to follow a specially crafted URL that is designed to cause Cisco Webex Meetings to include a remote file in the web UI. A successful exploit could allow the attacker to cause the application to offer a remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-redirect-XuZFU3PH	A-CIS-WEBE-180621/38

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file to a user, which could allow the attacker to conduct further phishing or spoofing attacks. **CVE ID : CVE-2021-1525**		
Uncontrolled Search Path Element	04-Jun-21	6.9	A vulnerability in Cisco Webex Meetings Desktop App for Windows, Cisco Webex Meetings Server, Cisco Webex Network Recording Player for Windows, and Cisco Webex Teams for Windows could allow an authenticated, local attacker to perform a DLL injection attack on an affected device. To exploit this vulnerability, the attacker must have valid credentials on the Windows system. This vulnerability is due to incorrect handling of directory paths at run time. An attacker could exploit this vulnerability by inserting a configuration file in a specific path in the system, which can cause a malicious DLL file to be loaded when the application starts. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of another user account. **CVE ID : CVE-2021-1536**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-dll-inject-XNmcSGTU	A-CIS-WEBE-180621/39
webex_meetings_server					
Improper Restriction of Operations	04-Jun-21	6.8	A vulnerability in Cisco Webex Network Recording Player for Windows and MacOS and Cisco Webex	https://tools.cisco.com/security/center/content/Cis	A-CIS-WEBE-180621/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Player for Windows and MacOS could allow an attacker to execute arbitrary code on an affected system. The vulnerability is due to insufficient validation of values within Webex recording files formatted as either Advanced Recording Format (ARF) or Webex Recording Format (WRF). An attacker could exploit the vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user. **CVE ID : CVE-2021-1502**	coSecurityAdvisory/cisco-sa-webex-player-dOJ2jOJ	
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	A vulnerability in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to redirect users to a malicious file. This vulnerability is due to improper validation of URL paths in the application interface. An attacker could exploit this vulnerability by persuading a user to follow a specially crafted URL that is designed to cause Cisco Webex Meetings to include a remote file in the web UI. A successful exploit could allow the attacker to cause the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-redirect-XuZFU3PH	A-CIS-WEBE-180621/41

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application to offer a remote file to a user, which could allow the attacker to conduct further phishing or spoofing attacks. **CVE ID : CVE-2021-1525**		
Uncontrolled Search Path Element	04-Jun-21	6.9	A vulnerability in Cisco Webex Meetings Desktop App for Windows, Cisco Webex Meetings Server, Cisco Webex Network Recording Player for Windows, and Cisco Webex Teams for Windows could allow an authenticated, local attacker to perform a DLL injection attack on an affected device. To exploit this vulnerability, the attacker must have valid credentials on the Windows system. This vulnerability is due to incorrect handling of directory paths at run time. An attacker could exploit this vulnerability by inserting a configuration file in a specific path in the system, which can cause a malicious DLL file to be loaded when the application starts. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of another user account. **CVE ID : CVE-2021-1536**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-dll-inject-XNmcSGTU	A-CIS-WEBE-180621/42
webex_network_recording_player					
Improper Restriction of	04-Jun-21	6.8	A vulnerability in Cisco Webex Network Recording Player for Windows and	https://tools.cisco.com/security/center	A-CIS-WEBE-180621/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			MacOS and Cisco Webex Player for Windows and MacOS could allow an attacker to execute arbitrary code on an affected system. The vulnerability is due to insufficient validation of values within Webex recording files formatted as either Advanced Recording Format (ARF) or Webex Recording Format (WRF). An attacker could exploit the vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user. **CVE ID : CVE-2021-1502**	/content/CiscoSecurityAdvisory/cisco-sa-webex-player-dOJ2jOJ	
Uncontrolled Search Path Element	04-Jun-21	6.9	A vulnerability in Cisco Webex Meetings Desktop App for Windows, Cisco Webex Meetings Server, Cisco Webex Network Recording Player for Windows, and Cisco Webex Teams for Windows could allow an authenticated, local attacker to perform a DLL injection attack on an affected device. To exploit this vulnerability, the attacker must have valid credentials on the Windows system. This vulnerability is due to incorrect handling of directory paths at run time.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-dll-inject-XNmcSGTU	A-CIS-WEBE-180621/44

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by inserting a configuration file in a specific path in the system, which can cause a malicious DLL file to be loaded when the application starts. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of another user account. **CVE ID : CVE-2021-1536**		
webex_player					
Out-of-bounds Write	04-Jun-21	5.8	A vulnerability in Cisco Webex Player for Windows and MacOS could allow an attacker to cause the affected software to terminate or to gain access to memory state information that is related to the vulnerable application. The vulnerability is due to insufficient validation of values in Webex recording files that are stored in Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a malicious WRF file to a user as a link or email attachment and then persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to crash the affected software and view memory state information. **CVE ID : CVE-2021-1527**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-player-kxtkFbnR	A-CIS-WEBE-180621/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
webex_teams					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Jun-21	6.8	A vulnerability in Cisco Webex Network Recording Player for Windows and MacOS and Cisco Webex Player for Windows and MacOS could allow an attacker to execute arbitrary code on an affected system. The vulnerability is due to insufficient validation of values within Webex recording files formatted as either Advanced Recording Format (ARF) or Webex Recording Format (WRF). An attacker could exploit the vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user. **CVE ID : CVE-2021-1502**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-player-dOJ2jOJ	A-CIS-WEBE-180621/46
Uncontrolled Search Path Element	04-Jun-21	6.9	A vulnerability in Cisco Webex Meetings Desktop App for Windows, Cisco Webex Meetings Server, Cisco Webex Network Recording Player for Windows, and Cisco Webex Teams for Windows could allow an authenticated, local attacker to perform a DLL injection attack on an affected device. To exploit this vulnerability, the attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-dll-inject-XNmcSGTU	A-CIS-WEBE-180621/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must have valid credentials on the Windows system. This vulnerability is due to incorrect handling of directory paths at run time. An attacker could exploit this vulnerability by inserting a configuration file in a specific path in the system, which can cause a malicious DLL file to be loaded when the application starts. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of another user account. **CVE ID : CVE-2021-1536**		
Ckeditor					
ckeditor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-21	4.3	A cross-site scripting (XSS) vulnerability in the HTML Data Processor in CKEditor 4 4.14.0 through 4.16.x before 4.16.1 allows remote attackers to inject executable JavaScript code through a crafted comment because --!> is mishandled. **CVE ID : CVE-2021-33829**	https://ckeditor.com/blog/ckeditor-4.16.1-with-accessibility-enhancements/#improvements-for-comments-in-html-parser	A-CKE-CKED-180621/48
clogica					
wp_login_security_and_history					
Cross-Site Request Forgery (CSRF)	01-Jun-21	3.5	The WP Login Security and History WordPress plugin through 1.0 did not have CSRF check when saving its settings, not any sanitisation or validation on them. This	https://wpscan.com/vulnerability/eeb41d7b-8f9e-4a12-b65f-f310f08e4ac	A-CLO-WP_L-180621/49

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow attackers to make logged in administrators change the plugin's settings to arbitrary values, and set XSS payloads on them as well **CVE ID : CVE-2021-24328**	e	
cloverdx					
cloverdx					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-21	4.3	A cross-site scripting (XSS) vulnerability in CloverDX Server 5.9.0, CloverDX 5.8.1, CloverDX 5.7.0, and earlier allows remote attackers to inject arbitrary web script or HTML via the sessionToken parameter of multiple methods in Simple HTTP API. This is resolved in 5.9.1 and 5.10. **CVE ID : CVE-2021-30133**	https://support1.cloverdx.com/hc/en-us/articles/360021006520, https://support.cloverdx.com/releases/	A-CLO-CLOV-180621/50
connekthq					
instant_images_-_one_click_unsplash_uploads					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	The Instant Images â€“ One Click Unsplash Uploads WordPress plugin before 4.4.0.1 did not properly validate and sanitise its unsplash_download_w and unsplash_download_h parameter settings (/wp-admin/upload.php?page=instant-images), only validating them client side before saving them, leading to a Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24334**	https://wpscan.com/vulnerability/ae79189a-6b63-4110-9567-cd7c97d71e4f	A-CON-INST-180621/51
content_copy_protection_\\&_prevent_image_save_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
datasette					
datasette					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-21	4.3	Datasette is an open source multi-tool for exploring and publishing data. The `?_trace=1` debugging feature in Datasette does not correctly escape generated HTML, resulting in a [reflected cross-site scripting](https://owasp.org/www-community/attacks/xss/#reflected-xss-attacks) vulnerability. This vulnerability is particularly relevant if your Datasette installation includes authenticated features using plugins such as [datasette-auth-passwords](https://datasette.io/plugins/datasette-auth-passwords) as an attacker could use the vulnerability to access protected data. Datasette 0.57 and 0.56.1 both include patches for this issue. If you run Datasette behind a proxy you can workaround this issue by rejecting any incoming requests with `?_trace=` or `&_trace=` in their query string parameters. **CVE ID : CVE-2021-32670**	https://datasette.io/plugins/datasette-auth-passwords, https://github.com/simonw/datasette/security/advisories/GHSA-xw7c-jx9m-xh5g, https://github.com/simonw/datasette/issues/1360	A-DAT-DATA-180621/52
deliciousbrains					
database_backup					
Improper	01-Jun-21	3.5	The Database Backup for	https://wpsc	A-DEL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			WordPress plugin before 2.4 did not escape the backup_recipient POST parameter in before output it back in the attribute of an HTML tag, leading to a Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24322**	an.com/vulnerability/6bea6301-0762-45c3-a4eb-15d6ac4f9f37	DATA-180621/53
Dino					
dino					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jun-21	5	Dino before 0.1.2 and 0.2.x before 0.2.1 allows Directory Traversal (only for creation of new files) via URI-encoded path separators. **CVE ID : CVE-2021-33896**	https://dino.im/security/cve-2021-33896/, https://dino.im/blog/, http://www.openwall.com/lists/oss-security/2021/06/07/2	A-DIN-DINO-180621/54
easy_preloader_project					
easy_preloader					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-21	3.5	The Easy Preloader WordPress plugin through 1.0.0 does not sanitise its setting fields, leading to authenticated (admin+) Stored Cross-Site scripting issues **CVE ID : CVE-2021-24344**	https://wpscan.com/vulnerability/6d6c1d46-5c3d-4d56-9728-2f94064132aa	A-EAS-EASY-180621/55
Entrouvert					
lasso					
Improper Verification of Cryptographi	04-Jun-21	5	Lasso all versions prior to 2.7.0 has improper verification of a cryptographic signature.	https://git.entrouvert.org/lasso.git/commit/?id=076a37d7f0eb	A-ENT-LASS-180621/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c Signature			**CVE ID : CVE-2021-28091**	7400112748 1da2d35568 3693cde9, https://git.e ntrouvert.or g/lasso.git/tr ee/NEWS?id =v2.7.0	
Esri					
arcgis_server					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	07-Jun-21	5	A SQL injection vulnerability exists in some configurations of ArcGIS Server versions 10.8.1 and earlier. Specially crafted web requests can expose information that is not intended to be disclosed (not customer datasets). Web Services that use file based data sources (file Geodatabase or Shape Files or tile cached services) are unaffected by this issue. **CVE ID : CVE-2021-29099**	https://ww w.esri.com/a rcgis-blog/product s/arcgis-enterprise/a dministratio n/security-advisory-e21-03-server-sql/	A-ESR-ARCG-180621/57
external_media_project					
external_media					
Unrestricted Upload of File with Dangerous Type	01-Jun-21	6.5	The wp_ajax_upload-remote-file AJAX action of the External Media WordPress plugin before 1.0.34 was vulnerable to arbitrary file uploads via any authenticated users. **CVE ID : CVE-2021-24311**	https://wpsc an.com/vuln erability/4fb 90999-6f91-4200-a0cc-bfe9b34a5de 9	A-EXT-EXTE-180621/58
F5					
nginx_controller					
Cleartext Transmissio	01-Jun-21	5.8	Intra-cluster communication does not use TLS. The	https://supp ort.f5.com/cs	A-F5-NGIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Sensitive Information			services within the NGINX Controller 3.x before 3.4.0 namespace are using cleartext protocols inside the cluster. **CVE ID : CVE-2021-23018**	p/article/K97002210	180621/59
Insufficiently Protected Credentials	01-Jun-21	6.9	The NGINX Controller 2.0.0 thru 2.9.0 and 3.x before 3.15.0 Administrator password may be exposed in the systemd.txt file that is included in the NGINX support package. **CVE ID : CVE-2021-23019**	https://support.f5.com/csp/article/K04884013	A-F5-NGIN-180621/60
Use of Insufficiently Random Values	01-Jun-21	2.1	The NAAS 3.x before 3.10.0 API keys were generated using an insecure pseudo-random string and hashing algorithm which could lead to predictable keys. **CVE ID : CVE-2021-23020**	https://support.f5.com/csp/article/K45263486	A-F5-NGIN-180621/61
Incorrect Permission Assignment for Critical Resource	01-Jun-21	2.1	The Nginx Controller 3.x before 3.7.0 agent configuration file /etc/controller-agent/agent.conf is world readable with current permission bits set to 644. **CVE ID : CVE-2021-23021**	https://support.f5.com/csp/article/K36926027	A-F5-NGIN-180621/62
Ffmpeg					
ffmpeg					
Improper Validation of Array Index	03-Jun-21	6.8	dwa_uncompress in libavcodec/exr.c in FFmpeg 4.4 allows an out-of-bounds array access because dc_count is not strictly checked.	https://github.com/FFmpeg/FFmpeg/commit/26d3c81bc5ef2f8c3f09d45eaeacfb4b1139	A-FFM-FFMP-180621/63

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-33815	a777	
flask-appbuilder_project					
flask-appbuilder					
Observable Discrepancy	07-Jun-21	5	Flask-AppBuilder is a development framework, built on top of Flask. User enumeration in database authentication in Flask-AppBuilder <= 3.2.3. Allows for a non authenticated user to enumerate existing accounts by timing the response time from the server when you are logging in. Upgrade to version 3.3.0 or higher to resolve. **CVE ID : CVE-2021-29621**	https://github.com/dpgaspar/Flask-AppBuilder/commit/780bd0e8fbf2d36ada52edb769477e0a4edae580, https://github.com/dpgaspar/Flask-AppBuilder/security/advisories/GHSA-434h-p4gx-jm89	A-FLA-FLAS-180621/64
forms_project					
forms					
N/A	01-Jun-21	5	The package forms before 1.2.1, from 1.3.0 and before 1.3.2 are vulnerable to Regular Expression Denial of Service (ReDoS) via email validation. **CVE ID : CVE-2021-23388**	https://github.com/caolan/forms/pull/214/commits/d4bd5b5febfe49c1f585f162e04ec810f8dc47a0, https://snyk.io/vuln/SNYK-JS-FORMS-1296389	A-FOR-FORM-180621/65
Fortinet					
fortiproxy					
Out-of-bounds	03-Jun-21	4	A stack-based buffer overflow vulnerability in FortiProxy	https://fortiguard.com/a	A-FOR-FORT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			physical appliance CLI 2.0.0 to 2.0.1, 1.2.0 to 1.2.9, 1.1.0 to 1.1.6, 1.0.0 to 1.0.7 may allow an authenticated, remote attacker to perform a Denial of Service attack by running the `diagnose sys cpuset` with a large cpuset mask value. Fortinet is not aware of any successful exploitation of this vulnerability that would lead to code execution. **CVE ID : CVE-2021-22130**	dvisory/FG-IR-21-006	180621/66
fortiweb					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jun-21	9	An OS command injection vulnerability in FortiWeb's management interface 6.3.7 and below, 6.2.3 and below, 6.1.x, 6.0.x, 5.9.x may allow a remote authenticated attacker to execute arbitrary commands on the system via the SAML server configuration page. **CVE ID : CVE-2021-22123**	https://fortiguard.com/advisory/FG-IR-20-120	A-FOR-FORT-180621/67
Gitlab					
gitlab					
Exposure of Resource to Wrong Sphere	08-Jun-21	5	An information disclosure vulnerability in GitLab EE versions 13.11 and later allowed a project owner to leak information about the members' on-call rotations in other projects **CVE ID : CVE-2021-22215**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22215.json	A-GIT-GITL-180621/68
Uncontrolled Resource Consumption	08-Jun-21	4	A denial of service vulnerability in all versions of GitLab CE/EE before 13.12.2,	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-180621/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13.11.5 or 13.10.5 allows an attacker to cause uncontrolled resource consumption with a very long issue or merge request description **CVE ID : CVE-2021-22216**	/blob/master/2021/CVE-2021-22216.json	
Uncontrolled Resource Consumption	08-Jun-21	4	A denial of service vulnerability in all versions of GitLab CE/EE before 13.12.2, 13.11.5 or 13.10.5 allows an attacker to cause uncontrolled resource consumption with a specially crafted issue or merge request **CVE ID : CVE-2021-22217**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22217.json	A-GIT-GITL-180621/70
Insertion of Sensitive Information into Log File	08-Jun-21	4	GitLab CE/EE since version 9.5 allows a high privilege user to obtain sensitive information from log files because the sensitive information was not correctly registered for log masking. **CVE ID : CVE-2021-22219**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22219.json	A-GIT-GITL-180621/71
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-21	4.3	An issue has been discovered in GitLab affecting all versions starting with 13.10. GitLab was vulnerable to a stored XSS in blob viewer of notebooks. **CVE ID : CVE-2021-22220**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22220.json	A-GIT-GITL-180621/72
GNU					
binutils					
Uncontrolled Recursion	02-Jun-21	5	A flaw was discovered in GNU libiberty within demangle_path() in rust-	https://src.fedoraproject.org/rpms/bin	A-GNU-BINU-180621/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			demangle.c, as distributed in GNU Binutils version 2.36. A crafted symbol can cause stack memory to be exhausted leading to a crash. **CVE ID : CVE-2021-3530**	utils/blob/rawhide/f/binutils-CVE-2021-3530.patch	
go.uuid_project					
go.uuid					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	02-Jun-21	7.5	A flaw was found in github.com/satori/go.uuid in versions from commit 0ef6afb2f6cdd6cdaeee3885a95099c63f18fc8c to d91630c8510268e75203009fe7daf2b8e1d60c45. Due to insecure randomness in the g.rand.Read function the generated UUIDs are predictable for an attacker. **CVE ID : CVE-2021-3538**	N/A	A-GO.-GO.U-180621/74
Google					
chrome					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Jun-21	6.8	Incorrect security UI in Web App Installs in Google Chrome on Android prior to 90.0.4430.212 allowed an attacker who convinced a user to install a web application to inject scripts or HTML into a privileged page via a crafted HTML page. **CVE ID : CVE-2021-30506**	https://crbug.com/1180126, https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html	A-GOO-CHRO-180621/75
Inclusion of Functionality from Untrusted Control	04-Jun-21	6.8	Inappropriate implementation in Offline in Google Chrome on Android prior to 90.0.4430.212 allowed a remote attacker	https://chromereleases.googleblog.com/2021/05/stable-	A-GOO-CHRO-180621/76

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			who had compromised the renderer process to bypass site isolation via a crafted HTML page. **CVE ID : CVE-2021-30507**	channel-update-for-desktop.html, https://crbug.com/1178202	
Out-of-bounds Write	04-Jun-21	6.8	Heap buffer overflow in Media Feeds in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to enable certain features in Chrome to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30508**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html, https://crbug.com/1195340	A-GOO-CHRO-180621/77
Out-of-bounds Write	04-Jun-21	6.8	Out of bounds write in Tab Strip in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page and a crafted Chrome extension. **CVE ID : CVE-2021-30509**	https://crbug.com/1196309, https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html	A-GOO-CHRO-180621/78
Use After Free	04-Jun-21	6.8	Use after free in Aura in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30510**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html	A-GOO-CHRO-180621/79
Out-of-bounds Read	04-Jun-21	5.8	Out of bounds read in Tab Groups in Google Chrome	https://chromereleases.g	A-GOO-CHRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted HTML page. **CVE ID : CVE-2021-30511**	oogleblog.com/2021/05/stable-channel-update-for-desktop.html	180621/80
Use After Free	04-Jun-21	6.8	Use after free in Notifications in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30512**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html	A-GOO-CHRO-180621/81
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jun-21	6.8	Type confusion in V8 in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30513**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html	A-GOO-CHRO-180621/82
Use After Free	04-Jun-21	6.8	Use after free in Autofill in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30514**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html	A-GOO-CHRO-180621/83
Use After Free	04-Jun-21	6.8	Use after free in File API in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a	https://chromereleases.googleblog.com/2021/05/stable-	A-GOO-CHRO-180621/84

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted HTML page. **CVE ID : CVE-2021-30515**	channel-update-for-desktop.html	
Out-of-bounds Write	04-Jun-21	6.8	Heap buffer overflow in History in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30516**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html	A-GOO-CHRO-180621/85
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jun-21	6.8	Type confusion in V8 in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30517**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html	A-GOO-CHRO-180621/86
Out-of-bounds Write	04-Jun-21	6.8	Heap buffer overflow in Reader Mode in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30518**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html	A-GOO-CHRO-180621/87
Use After Free	04-Jun-21	6.8	Use after free in Payments in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious payments app to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30519**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html	A-GOO-CHRO-180621/88

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	04-Jun-21	6.8	Use after free in Tab Strip in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30520**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html	A-GOO-CHRO-180621/89
Out-of-bounds Write	07-Jun-21	6.8	Heap buffer overflow in Autofill in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. **CVE ID : CVE-2021-30521**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/90
Use After Free	07-Jun-21	6.8	Use after free in WebAudio in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30522**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/91
Use After Free	07-Jun-21	6.8	Use after free in WebRTC in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit heap corruption via a crafted SCTP packet. **CVE ID : CVE-2021-30523**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/92
Use After Free	07-Jun-21	6.8	Use after free in TabStrip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a	https://chromereleases.googleblog.com/2021/05/	A-GOO-CHRO-180621/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30524**	stable-channel-update-for-desktop_25.html	
Use After Free	07-Jun-21	6.8	Use after free in TabGroups in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30525**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/94
Out-of-bounds Write	07-Jun-21	6.8	Out of bounds write in TabStrip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page. **CVE ID : CVE-2021-30526**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/95
Use After Free	07-Jun-21	6.8	Use after free in WebUI in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30527**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/96
Use After Free	07-Jun-21	6.8	Use after free in WebAuthentication in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker who had compromised the renderer process of a user who had	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-	A-GOO-CHRO-180621/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			saved a credit card in their Google account to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30528**	desktop_25.html	
Use After Free	07-Jun-21	6.8	Use after free in Bookmarks in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30529**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/98
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-Jun-21	6.8	Out of bounds memory access in WebAudio in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. **CVE ID : CVE-2021-30530**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/99
Incorrect Authorization	07-Jun-21	4.3	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2021-30531**	https://crbug.com/1115628, https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/100
Incorrect Authorization	07-Jun-21	4.3	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 91.0.4472.77	https://crbug.com/1117687, https://chro	A-GOO-CHRO-180621/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2021-30532**	mereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	
Incorrect Authorization	07-Jun-21	4.3	Insufficient policy enforcement in PopupBlocker in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass navigation restrictions via a crafted iframe. **CVE ID : CVE-2021-30533**	https://crbug.com/1145553, https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/102
Incorrect Authorization	07-Jun-21	4.3	Insufficient policy enforcement in iFrameSandbox in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2021-30534**	https://crbug.com/1151507, https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/103
Double Free	07-Jun-21	6.8	Double free in ICU in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30535**	https://crbug.com/1194899, https://chromereleases.googleblog.com/2021/05/stable-	A-GOO-CHRO-180621/104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				channel-update-for-desktop_25.html	
Out-of-bounds Read	07-Jun-21	5.8	Out of bounds read in V8 in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page. **CVE ID : CVE-2021-30536**	https://crbug.com/1194358, https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/105
Incorrect Authorization	07-Jun-21	4.3	Insufficient policy enforcement in cookies in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass cookie policy via a crafted HTML page. **CVE ID : CVE-2021-30537**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html, https://crbug.com/830101	A-GOO-CHRO-180621/106
Incorrect Authorization	07-Jun-21	4.3	Insufficient policy enforcement in content security policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2021-30538**	https://crbug.com/1115045, https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	07-Jun-21	5.8	Insufficient policy enforcement in content security policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2021-30539**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/108
Improper Input Validation	07-Jun-21	4.3	Incorrect security UI in payments in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker to perform domain spoofing via a crafted HTML page. **CVE ID : CVE-2021-30540**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/109
Use After Free	07-Jun-21	6.8	Use after free in Tab Strip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30542**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/110
Use After Free	07-Jun-21	6.8	Use after free in Tab Strip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30543**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-180621/111
goprayer					
wp_prayer					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	The WP Prayer WordPress plugin before 1.6.2 provides the functionality to store requested prayers/praises and list them on a WordPress website. These stored prayer/praise requests can be listed by using the WP Prayer engine. An authenticated WordPress user with any role can fill in the form to request a prayer. The form to request prayers or praises have several fields. The 'prayer request' and 'praise request' fields do not use proper input validation and can be used to store XSS payloads. **CVE ID : CVE-2021-24313**	https://wpscan.com/vulnerability/c7ab736d-27c4-4ec5-9681-a3f0dda86586	A-GOP-WP_P-180621/112
gstreamer_project					
gstreamer					
Out-of-bounds Read	02-Jun-21	4.3	GStreamer before 1.18.4 may perform an out-of-bounds read when handling certain ID3v2 tags. **CVE ID : CVE-2021-3522**	N/A	A-GST-GSTR-180621/113
HP					
oneview_for_vmware_vcenter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-21	4.3	A security vulnerability in HPE OneView for VMware vCenter (OV4VC) could be exploited remotely to allow Cross-Site Scripting. HPE has released the following software update to resolve the vulnerability in HPE OneView for VMware vCenter	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn04151en_us	A-HP-ONEV-180621/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(OV4VC). **CVE ID : CVE-2021-26584**		
Huawei					
emui					
N/A	03-Jun-21	2.1	There is a Business Logic Errors vulnerability in Huawei Smartphone. The malicious apps installed on the device can keep taking screenshots in the background. This issue does not cause system errors, but may cause personal information leakage. **CVE ID : CVE-2021-22308**	https://consumer.huawei.com/en/support/bulletin/2021/2/	A-HUA-EMUI-180621/115
N/A	03-Jun-21	5	There is a Security Function vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality. **CVE ID : CVE-2021-22313**	https://consumer.huawei.com/en/support/bulletin/2021/2/	A-HUA-EMUI-180621/116
Missing Authentication for Critical Function	03-Jun-21	4.6	There is a Missing Authentication for Critical Function vulnerability in Huawei Smartphone. Attackers with physical access to the device can thereby exploit this vulnerability. A successful exploitation of this vulnerability can compromise the device's data security and functional availability. **CVE ID : CVE-2021-22316**	https://consumer.huawei.com/en/support/bulletin/2021/2/	A-HUA-EMUI-180621/117
N/A	03-Jun-21	5	There is an Information Disclosure vulnerability in Huawei Smartphone.	https://consumer.huawei.com/en/sup	A-HUA-EMUI-180621/118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability may impair data confidentiality. **CVE ID : CVE-2021-22317**	port/bulletin/2021/2/	
Missing Authentication for Critical Function	03-Jun-21	5	There is a Missing Authentication for Critical Function vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality. **CVE ID : CVE-2021-22322**	https://consumer.huawei.com/en/support/bulletin/2021/3/	A-HUA-EMUI-180621/119
Insufficiently Protected Credentials	03-Jun-21	5	There is a Credentials Management Errors vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality. **CVE ID : CVE-2021-22324**	https://consumer.huawei.com/en/support/bulletin/2021/3/	A-HUA-EMUI-180621/120
Cleartext Transmission of Sensitive Information	03-Jun-21	5	There is an Information Disclosure vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may result in video streams being intercepted during transmission. **CVE ID : CVE-2021-22325**	https://consumer.huawei.com/en/support/bulletin/2021/3/	A-HUA-EMUI-180621/121
Improper Validation of Array Index	03-Jun-21	10	There is an Improper Validation of Array Index vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause code to execute, thus obtaining system permissions. **CVE ID : CVE-2021-22333**	https://consumer.huawei.com/en/support/bulletin/2021/4/	A-HUA-EMUI-180621/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	03-Jun-21	3.3	There is an Improper Access Control vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause app redirections. **CVE ID : CVE-2021-22334**	https://consumer.huawei.com/en/support/bulletin/2021/4/	A-HUA-EMUI-180621/123
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Jun-21	4.6	There is a Memory Buffer Improper Operation Limit vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause exceptions in image processing. **CVE ID : CVE-2021-22335**	https://consumer.huawei.com/en/support/bulletin/2021/4/	A-HUA-EMUI-180621/124
Improper Control of Generation of Code ('Code Injection')	03-Jun-21	5	There is an Improper Control of Generation of Code vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause denial of security services on a rooted device. **CVE ID : CVE-2021-22336**	https://consumer.huawei.com/en/support/bulletin/2021/4/	A-HUA-EMUI-180621/125
N/A	03-Jun-21	5	There is an Information Disclosure vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause leaking of user click data. **CVE ID : CVE-2021-22337**	https://consumer.huawei.com/en/support/bulletin/2021/4/	A-HUA-EMUI-180621/126
magic_ui					
N/A	03-Jun-21	2.1	There is a Business Logic Errors vulnerability in Huawei Smartphone. The malicious apps installed on the device can keep taking	https://consumer.huawei.com/en/support/bulletin/2021/2/	A-HUA-MAGI-180621/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			screenshots in the background. This issue does not cause system errors, but may cause personal information leakage. **CVE ID : CVE-2021-22308**		
N/A	03-Jun-21	5	There is a Security Function vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality. **CVE ID : CVE-2021-22313**	https://consumer.huawei.com/en/support/bulletin/2021/2/	A-HUA-MAGI-180621/128
Missing Authentication for Critical Function	03-Jun-21	4.6	There is a Missing Authentication for Critical Function vulnerability in Huawei Smartphone. Attackers with physical access to the device can thereby exploit this vulnerability. A successful exploitation of this vulnerability can compromise the device's data security and functional availability. **CVE ID : CVE-2021-22316**	https://consumer.huawei.com/en/support/bulletin/2021/2/	A-HUA-MAGI-180621/129
N/A	03-Jun-21	5	There is an Information Disclosure vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality. **CVE ID : CVE-2021-22317**	https://consumer.huawei.com/en/support/bulletin/2021/2/	A-HUA-MAGI-180621/130
Missing Authentication for Critical Function	03-Jun-21	5	There is a Missing Authentication for Critical Function vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data	https://consumer.huawei.com/en/support/bulletin/2021/3/	A-HUA-MAGI-180621/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			confidentiality. **CVE ID : CVE-2021-22322**		
Insufficiently Protected Credentials	03-Jun-21	5	There is a Credentials Management Errors vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality. **CVE ID : CVE-2021-22324**	https://consumer.huawei.com/en/support/bulletin/2021/3/	A-HUA-MAGI-180621/132
Cleartext Transmission of Sensitive Information	03-Jun-21	5	There is an Information Disclosure vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may result in video streams being intercepted during transmission. **CVE ID : CVE-2021-22325**	https://consumer.huawei.com/en/support/bulletin/2021/3/	A-HUA-MAGI-180621/133
Improper Validation of Array Index	03-Jun-21	10	There is an Improper Validation of Array Index vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause code to execute, thus obtaining system permissions. **CVE ID : CVE-2021-22333**	https://consumer.huawei.com/en/support/bulletin/2021/4/	A-HUA-MAGI-180621/134
Incorrect Authorization	03-Jun-21	3.3	There is an Improper Access Control vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause app redirections. **CVE ID : CVE-2021-22334**	https://consumer.huawei.com/en/support/bulletin/2021/4/	A-HUA-MAGI-180621/135
Improper Restriction of	03-Jun-21	4.6	There is a Memory Buffer Improper Operation Limit vulnerability in Huawei	https://consumer.huawei.com/en/sup	A-HUA-MAGI-180621/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Smartphone. Successful exploitation of this vulnerability may cause exceptions in image processing. **CVE ID : CVE-2021-22335**	port/bulletin/2021/4/	
Improper Control of Generation of Code ('Code Injection')	03-Jun-21	5	There is an Improper Control of Generation of Code vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause denial of security services on a rooted device. **CVE ID : CVE-2021-22336**	https://consumer.huawei.com/en/support/bulletin/2021/4/	A-HUA-MAGI-180621/137
N/A	03-Jun-21	5	There is an Information Disclosure vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause leaking of user click data. **CVE ID : CVE-2021-22337**	https://consumer.huawei.com/en/support/bulletin/2021/4/	A-HUA-MAGI-180621/138
IBM					
application_gateway					
Insecure Storage of Sensitive Information	01-Jun-21	2.1	IBM Security Verify Access 20.07 allows web pages to be stored locally which can be read by another user on the system. X-Force ID: 199278. **CVE ID : CVE-2021-20575**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199278, https://www.ibm.com/support/pages/node/6457315	A-IBM-APPL-180621/139
N/A	01-Jun-21	5	IBM Security Verify Access 20.07 could allow a remote attacker to send a specially crafted HTTP GET request	https://exchange.xforce.ibmcloud.com/vulnerabiliti	A-IBM-APPL-180621/140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that could cause the application to crash. **CVE ID : CVE-2021-20576**	es/199280, https://www.ibm.com/support/pages/node/6457315	
collaborative_lifecycle_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199406. **CVE ID : CVE-2021-29668**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199406	A-IBM-COLL-180621/141
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199408. **CVE ID : CVE-2021-29670**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199408	A-IBM-COLL-180621/142
Improper Neutralization of Input During Web Page Generation	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in	https://www.ibm.com/support/pages/node/6457739, https://exch	A-IBM-COLL-180621/143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194449. **CVE ID : CVE-2021-20338**	ange.xforce.ibmcloud.com/vulnerabilities/194449	
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194593. **CVE ID : CVE-2021-20343**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194593	A-IBM-COLL-180621/144
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194594. **CVE ID : CVE-2021-20345**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194594	A-IBM-COLL-180621/145
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send	https://www.ibm.com/support/pages/node/6457739, https://exch	A-IBM-COLL-180621/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194595. **CVE ID : CVE-2021-20346**	ange.xforce.ibmcloud.com/vulnerabilities/194595	
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194596. **CVE ID : CVE-2021-20347**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194596	A-IBM-COLL-180621/147
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-ForceID: 194597. **CVE ID : CVE-2021-20348**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194597	A-IBM-COLL-180621/148
Generation of Error Message Containing Sensitive Information	02-Jun-21	4	IBM Jazz Foundation and IBM Engineering products could allow a remote attacker to obtain sensitive information when an error message is returned in the browser. This	https://www.ibm.com/support/pages/node/6457739, https://exch	A-IBM-COLL-180621/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information could be used in further attacks against the system. IBM X-Force ID: 195516. **CVE ID : CVE-2021-20371**	ange.xforce.ibmcloud.com/vulnerabilities/195516	
engineering_lifecycle_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199406. **CVE ID : CVE-2021-29668**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199406	A-IBM-ENGI-180621/150
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199408. **CVE ID : CVE-2021-29670**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199408	A-IBM-ENGI-180621/151
Improper Neutralization of Input During Web Page Generation ('Cross-site	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.i	A-IBM-ENGI-180621/152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194449. **CVE ID : CVE-2021-20338**	bmcloud.com/vulnerabilities/194449	
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194593. **CVE ID : CVE-2021-20343**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194593	A-IBM-ENGI-180621/153
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194594. **CVE ID : CVE-2021-20345**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194594	A-IBM-ENGI-180621/154
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.i	A-IBM-ENGI-180621/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194595. **CVE ID : CVE-2021-20346**	bmcloud.com/vulnerabilities/194595	
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194596. **CVE ID : CVE-2021-20347**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194596	A-IBM-ENGI-180621/156
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-ForceID: 194597. **CVE ID : CVE-2021-20348**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194597	A-IBM-ENGI-180621/157
Generation of Error Message Containing Sensitive Information	02-Jun-21	4	IBM Jazz Foundation and IBM Engineering products could allow a remote attacker to obtain sensitive information when an error message is returned in the browser. This information could be used in	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.i	A-IBM-ENGI-180621/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			further attacks against the system. IBM X-Force ID: 195516. **CVE ID : CVE-2021-20371**	bmcloud.com/vulnerabilities/195516	
engineering_lifecycle_optimization_-_engineering_insights					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199406. **CVE ID : CVE-2021-29668**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199406	A-IBM-ENGI-180621/159
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199408. **CVE ID : CVE-2021-29670**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199408	A-IBM-ENGI-180621/160
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com	A-IBM-ENGI-180621/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194449. **CVE ID : CVE-2021-20338**	/vulnerabilities/194449	
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194593. **CVE ID : CVE-2021-20343**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194593	A-IBM-ENGI-180621/162
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194594. **CVE ID : CVE-2021-20345**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194594	A-IBM-ENGI-180621/163
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com	A-IBM-ENGI-180621/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194595. **CVE ID : CVE-2021-20346**	/vulnerabilities/194595	
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194596. **CVE ID : CVE-2021-20347**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194596	A-IBM-ENGI-180621/165
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-ForceID: 194597. **CVE ID : CVE-2021-20348**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194597	A-IBM-ENGI-180621/166
Generation of Error Message Containing Sensitive Information	02-Jun-21	4	IBM Jazz Foundation and IBM Engineering products could allow a remote attacker to obtain sensitive information when an error message is returned in the browser. This information could be used in further attacks against the	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com	A-IBM-ENGI-180621/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system. IBM X-Force ID: 195516. **CVE ID : CVE-2021-20371**	/vulnerabilities/195516	
engineering_lifecycle_optimization_-_publishing					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199406. **CVE ID : CVE-2021-29668**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199406	A-IBM-ENGI-180621/168
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199408. **CVE ID : CVE-2021-29670**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199408	A-IBM-ENGI-180621/169
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabiliti	A-IBM-ENGI-180621/170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials disclosure within a trusted session. IBM X-Force ID: 194449. **CVE ID : CVE-2021-20338**	es/194449	
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194593. **CVE ID : CVE-2021-20343**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194593	A-IBM-ENGI-180621/171
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194594. **CVE ID : CVE-2021-20345**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194594	A-IBM-ENGI-180621/172
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabiliti	A-IBM-ENGI-180621/173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enumeration or facilitating other attacks. IBM X-Force ID: 194595. **CVE ID : CVE-2021-20346**	es/194595	
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194596. **CVE ID : CVE-2021-20347**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194596	A-IBM-ENGI-180621/174
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-ForceID: 194597. **CVE ID : CVE-2021-20348**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194597	A-IBM-ENGI-180621/175
Generation of Error Message Containing Sensitive Information	02-Jun-21	4	IBM Jazz Foundation and IBM Engineering products could allow a remote attacker to obtain sensitive information when an error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID:	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabiliti	A-IBM-ENGI-180621/176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			195516. **CVE ID : CVE-2021-20371**	es/195516	
engineering_test_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199406. **CVE ID : CVE-2021-29668**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199406	A-IBM-ENGI-180621/177
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199408. **CVE ID : CVE-2021-29670**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199408	A-IBM-ENGI-180621/178
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194449	A-IBM-ENGI-180621/179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a trusted session. IBM X-Force ID: 194449. **CVE ID : CVE-2021-20338**		
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194593. **CVE ID : CVE-2021-20343**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194593	A-IBM-ENGI-180621/180
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194594. **CVE ID : CVE-2021-20345**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194594	A-IBM-ENGI-180621/181
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194595	A-IBM-ENGI-180621/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			other attacks. IBM X-Force ID: 194595. **CVE ID : CVE-2021-20346**		
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194596. **CVE ID : CVE-2021-20347**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194596	A-IBM-ENGI-180621/183
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-ForceID: 194597. **CVE ID : CVE-2021-20348**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194597	A-IBM-ENGI-180621/184
Generation of Error Message Containing Sensitive Information	02-Jun-21	4	IBM Jazz Foundation and IBM Engineering products could allow a remote attacker to obtain sensitive information when an error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 195516.	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/195516	A-IBM-ENGI-180621/185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20371		
qradar_advisor_with_watson					
N/A	03-Jun-21	5	IBM QRadar Advisor With Watson App 1.1 through 2.5 as used on IBM QRadar SIEM 7.4 could allow a remote user to obtain sensitive information from HTTP requests that could aid in further attacks against the system. IBM X-Force ID: 195712. **CVE ID : CVE-2021-20380**	https://exchange.xforce.ibmcloud.com/vulnerabilities/195712, https://www.ibm.com/support/pages/node/6457941	A-IBM-QRAD-180621/186
rational_doors_next_generation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199406. **CVE ID : CVE-2021-29668**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199406	A-IBM-RATI-180621/187
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199408.	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199408	A-IBM-RATI-180621/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29670		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 194449. **CVE ID : CVE-2021-20338**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194449	A-IBM-RATI-180621/189
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194593. **CVE ID : CVE-2021-20343**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194593	A-IBM-RATI-180621/190
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194594.	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194594	A-IBM-RATI-180621/191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20345		
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194595. **CVE ID : CVE-2021-20346**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194595	A-IBM-RATI-180621/192
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194596. **CVE ID : CVE-2021-20347**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194596	A-IBM-RATI-180621/193
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-ForceID: 194597.	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194597	A-IBM-RATI-180621/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20348		
Generation of Error Message Containing Sensitive Information	02-Jun-21	4	IBM Jazz Foundation and IBM Engineering products could allow a remote attacker to obtain sensitive information when an error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 195516. **CVE ID : CVE-2021-20371**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/195516	A-IBM-RATI-180621/195
rational_engineering_lifecycle_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199406. **CVE ID : CVE-2021-29668**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199406	A-IBM-RATI-180621/196
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199408. **CVE ID : CVE-2021-29670**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199408	A-IBM-RATI-180621/197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 194449. **CVE ID : CVE-2021-20338**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194449	A-IBM-RATI-180621/198
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194593. **CVE ID : CVE-2021-20343**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194593	A-IBM-RATI-180621/199
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194594. **CVE ID : CVE-2021-20345**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194594	A-IBM-RATI-180621/200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194595. **CVE ID : CVE-2021-20346**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194595	A-IBM-RATI-180621/201
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194596. **CVE ID : CVE-2021-20347**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194596	A-IBM-RATI-180621/202
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-ForceID: 194597. **CVE ID : CVE-2021-20348**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194597	A-IBM-RATI-180621/203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	02-Jun-21	4	IBM Jazz Foundation and IBM Engineering products could allow a remote attacker to obtain sensitive information when an error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 195516. **CVE ID : CVE-2021-20371**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/195516	A-IBM-RATI-180621/204
rational_quality_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199406. **CVE ID : CVE-2021-29668**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199406	A-IBM-RATI-180621/205
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199408. **CVE ID : CVE-2021-29670**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199408	A-IBM-RATI-180621/206
Improper	02-Jun-21	3.5	IBM Jazz Foundation and IBM	https://ww	A-IBM-RATI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			Engineering products are 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: 194449. **CVE ID : CVE-2021-20338**	w.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194449	180621/207
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194593. **CVE ID : CVE-2021-20343**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194593	A-IBM-RATI-180621/208
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194594. **CVE ID : CVE-2021-20345**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194594	A-IBM-RATI-180621/209
Server-Side	02-Jun-21	5.5	IBM Jazz Foundation and IBM	https://ww	A-IBM-RATI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (SSRF)			Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194595. **CVE ID : CVE-2021-20346**	w.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194595	180621/210
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194596. **CVE ID : CVE-2021-20347**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194596	A-IBM-RATI-180621/211
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-ForceID: 194597. **CVE ID : CVE-2021-20348**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194597	A-IBM-RATI-180621/212
Generation	02-Jun-21	4	IBM Jazz Foundation and IBM	https://ww	A-IBM-RATI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Error Message Containing Sensitive Information			Engineering products could allow a remote attacker to obtain sensitive information when an error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 195516. **CVE ID : CVE-2021-20371**	w.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/195516	180621/213
removable_media_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199406. **CVE ID : CVE-2021-29668**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199406	A-IBM-REMO-180621/214
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are 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: 199408. **CVE ID : CVE-2021-29670**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/199408	A-IBM-REMO-180621/215
Improper Neutralizatio	02-Jun-21	3.5	IBM Jazz Foundation and IBM Engineering products are	https://www.ibm.com/s	A-IBM-REMO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			vulnerable to cross-site scripting. 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: 194449. **CVE ID : CVE-2021-20338**	upport/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194449	180621/216
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194593. **CVE ID : CVE-2021-20343**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194593	A-IBM-REMO-180621/217
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194594. **CVE ID : CVE-2021-20345**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194594	A-IBM-REMO-180621/218
Server-Side Request	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are	https://www.ibm.com/s	A-IBM-REMO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194595. **CVE ID : CVE-2021-20346**	upport/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194595	180621/219
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194596. **CVE ID : CVE-2021-20347**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194596	A-IBM-REMO-180621/220
Server-Side Request Forgery (SSRF)	02-Jun-21	5.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-ForceID: 194597. **CVE ID : CVE-2021-20348**	https://www.ibm.com/support/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/194597	A-IBM-REMO-180621/221
Generation of Error	02-Jun-21	4	IBM Jazz Foundation and IBM Engineering products could	https://www.ibm.com/s	A-IBM-REMO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Message Containing Sensitive Information			allow a remote attacker to obtain sensitive information when an error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 195516. **CVE ID : CVE-2021-20371**	upport/pages/node/6457739, https://exchange.xforce.ibmcloud.com/vulnerabilities/195516	180621/222
security_verify_access					
Out-of-bounds Write	01-Jun-21	4.6	IBM Security Verify Access 20.07 is vulnerable to a stack based buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with elevated privileges. **CVE ID : CVE-2021-29665**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199399, https://www.ibm.com/support/pages/node/6457315	A-IBM-SECU-180621/223
Insecure Storage of Sensitive Information	01-Jun-21	2.1	IBM Security Verify Access 20.07 allows web pages to be stored locally which can be read by another user on the system. X-Force ID: 199278. **CVE ID : CVE-2021-20575**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199278, https://www.ibm.com/support/pages/node/6457315	A-IBM-SECU-180621/224
N/A	01-Jun-21	5	IBM Security Verify Access 20.07 could allow a remote attacker to send a specially crafted HTTP GET request that could cause the application to crash. **CVE ID : CVE-2021-20576**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199280, https://www.ibm.com/support/pages/node/6457	A-IBM-SECU-180621/225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				315	
Exposure of Sensitive Information to an Unauthorized Actor	01-Jun-21	5	IBM Security Verify Access 20.07 could disclose sensitive information in HTTP server headers that could be used in further attacks against the system. IBM X-Force ID: 199398. **CVE ID : CVE-2021-20585**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199398, https://www.ibm.com/support/pages/node/6457315	A-IBM-SECU-180621/226
spectrum_scale					
Use of Externally-Controlled Format String	01-Jun-21	7.2	IBM Spectrum Scale 5.0.0 through 5.0.5.6 and 5.1.0 through 5.1.0.3 system core component is affected by a format string security vulnerability. An attacker could execute arbitrary code in the context of process memory, potentially escalating their system privileges and taking control over the entire system with root access. IBM X-Force ID: 201474. **CVE ID : CVE-2021-29740**	https://www.ibm.com/support/pages/node/6457629, https://exchange.xforce.ibmcloud.com/vulnerabilities/201474	A-IBM-SPEC-180621/227
websphere_application_server_nd					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jun-21	6.5	IBM WebSphere Application Server Network Deployment 8.5 and 9.0 could allow a remote authenticated attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to read and delete arbitrary files on the system. IBM X-Force ID:	https://www.ibm.com/support/pages/node/6456955, https://exchange.xforce.ibmcloud.com/vulnerabilities/198435	A-IBM-WEBS-180621/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			198435. **CVE ID : CVE-2021-20517**		
icecoder					
icecoder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-21	3.5	In ICEcoder 8.0 allows, a reflected XSS vulnerability was identified in the multipe-results.php page due to insufficient sanitization of the _GET['replace'] variable. As a result, arbitrary Javascript code can get executed. **CVE ID : CVE-2021-32106**	N/A	A-ICE-ICEC-180621/229
iflychat					
iflychat					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-21	3.5	The iFlyChat - WordPress Chat plugin through 4.6.4 does not sanitise its APP ID setting before outputting it back in the page, leading to an authenticated Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24343**	https://wpscan.com/vulnerability/d6c72d90-e321-47b9-957a-6fea7c944293	A-IFL-IFLY-180621/230
in4velocity					
in4suite_erp					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Jun-21	6.4	SQL injection in In4Suite ERP 3.2.74.1370 allows attackers to modify or delete data, causing persistent changes to the application's content or behavior by using malicious SQL queries. **CVE ID : CVE-2021-27828**	https://www.in4velocity.com/in4suite-erp.html	A-IN4-IN4S-180621/231
inverse					
sogo					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Verification of Cryptographic Signature	04-Jun-21	5	SOGo 2.x before 2.4.1 and 3.x through 5.x before 5.1.1 does not validate the signatures of any SAML assertions it receives. Any actor with network access to the deployment could impersonate users when SAML is the authentication method. (Only versions after 2.0.5a are affected.) **CVE ID : CVE-2021-33054**	N/A	A-INV-SOGO-180621/232
jnews					
jnews					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-21	4.3	The JNews WordPress theme before 8.0.6 did not sanitise the cat_id parameter in the POST request /?ajax-request=jnews (with action=jnews_build_mega_category_*), leading to a Reflected Cross-Site Scripting (XSS) issue. **CVE ID : CVE-2021-24342**	https://wpscan.com/vulnerability/415ca763-fe65-48cb-acd3-b375a400217e	A-JNE-JNEW-180621/233
json_smart_project					
json_smart					
Out-of-bounds Write	01-Jun-21	5	A vulnerability was discovered in the indexOf function of JSONParserByteArray in JSON Smart versions 1.3 and 2.4 which causes a denial of service (DOS) via a crafted web request. **CVE ID : CVE-2021-31684**	https://github.com/netplex/json-smart-v1/pull/11, https://github.com/netplex/json-smart-v2/pull/68	A-JSO-JSON-180621/234
KDE					
messagelib					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	02-Jun-21	4	KDE Messagelib through 5.17.0 reveals cleartext of encrypted messages in some situations. Deleting an attachment of a decrypted encrypted message stored on a remote server (e.g., an IMAP server) causes KMail to upload the decrypted content of the message to the remote server. With a crafted message, a user could be tricked into decrypting an encrypted message and then deleting an attachment attached to this message. If the attacker has access to the messages stored on the email server, then the attacker could read the decrypted content of the encrypted message. This occurs in ViewerPrivate::deleteAttachment in messageviewer/src/viewer/viewer_p.cpp. **CVE ID : CVE-2021-31855**	https://kde.org/info/security/advisory-20210429-1.txt	A-KDE-MESS-180621/235
libtpms_project					
libtpms					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Jun-21	2.1	A stack corruption bug was found in libtpms in versions before 0.7.2 and before 0.8.0 while decrypting data using RSA. This flaw could result in a SIGBUS (bad memory access) and termination of swtpm. The highest threat from this vulnerability is to system availability.	https://bugzilla.redhat.com/show_bug.cgi?id=1964358	A-LIB-LIBT-180621/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-3569		
luca-app					
luca					
Exposure of Sensitive Information to an Unauthorized Actor	04-Jun-21	5	Luca through 1.7.4 on Android allows remote attackers to obtain sensitive information about COVID-19 tracking because requests related to Check-In State occur shortly after requests for Phone Number Registration. **CVE ID : CVE-2021-33838**	https://luca-app.de/securityoverview/properties/objectives.html	A-LUC-LUCA-180621/237
Exposure of Sensitive Information to an Unauthorized Actor	04-Jun-21	5	Luca through 1.7.4 on Android allows remote attackers to obtain sensitive information about COVID-19 tracking because the QR code of a Public Location can be intentionally confused with the QR code of a Private Meeting. **CVE ID : CVE-2021-33839**	https://luca-app.de/securityoverview/properties/objectives.html	A-LUC-LUCA-180621/238
Uncontrolled Resource Consumption	04-Jun-21	5	The server in Luca through 1.1.14 allows remote attackers to cause a denial of service (insertion of many fake records related to COVID-19) because Phone Number data lacks a digital signature. **CVE ID : CVE-2021-33840**	https://luca-app.de/securityoverview/processes/guest_registration.html#verifying-the-contact-data	A-LUC-LUCA-180621/239
lz4_project					
lz4					
Out-of-bounds Write	02-Jun-21	7.5	There's a flaw in lz4. An attacker who submits a crafted file to an application linked with lz4 may be able to	https://bugzilla.redhat.com/show_bug.cgi?id=1954	A-LZ4-LZ4-180621/240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			trigger an integer overflow, leading to calling of memmove() on a negative size argument, causing an out-of-bounds write and/or a crash. The greatest impact of this flaw is to availability, with some potential impact to confidentiality and integrity as well. **CVE ID : CVE-2021-3520**	559	
Mcafee					
agent					
Improper Privilege Management	10-Jun-21	2.1	Improper privilege management vulnerability in McAfee Agent for Windows prior to 5.7.3 allows a local user to modify event information in the MA event folder. This allows a local user to either add false events or remove events from the event logs prior to them being sent to the ePO server. **CVE ID : CVE-2021-31839**	https://kc.mcafee.com/corporate/index?page=content&id=SB10362	A-MCA-AGEN-180621/241
database_security					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-21	3.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows an administrator to embed JavaScript code when configuring the name of a database to be monitored. This would be triggered when any authorized user logs into the DBSec interface and	https://kc.mcafee.com/corporate/index?page=content&id=SB10359	A-MCA-DATA-180621/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			opens the properties configuration page for this database. **CVE ID : CVE-2021-31830**		
Deserialization of Untrusted Data	02-Jun-21	10	Deserialization of untrusted data vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows a remote unauthenticated attacker to create a reverse shell with administrator privileges on the DBSec server via carefully constructed Java serialized object sent to the DBSec server. **CVE ID : CVE-2021-23894**	https://kc.mcafee.com/corporate/index?page=content&id=SB10359	A-MCA-DATA-180621/243
Deserialization of Untrusted Data	02-Jun-21	9	Deserialization of untrusted data vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows a remote authenticated attacker to create a reverse shell with administrator privileges on the DBSec server via carefully constructed Java serialized object sent to the DBSec server. **CVE ID : CVE-2021-23895**	https://kc.mcafee.com/corporate/index?page=content&id=SB10359	A-MCA-DATA-180621/244
Cleartext Transmission of Sensitive Information	02-Jun-21	2.7	Cleartext Transmission of Sensitive Information vulnerability in the administrator interface of McAfee Database Security (DBSec) prior to 4.8.2 allows an administrator to view the unencrypted password of the McAfee Insights Server used to pass data to the Insights Server. This user is restricted	https://kc.mcafee.com/corporate/index?page=content&id=SB10359	A-MCA-DATA-180621/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to only have access to DBSec data in the Insights Server. **CVE ID : CVE-2021-23896**		
Microsoft					
365_apps					
N/A	08-Jun-21	6.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2021-31939**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31939	A-MIC-365_-180621/246
N/A	08-Jun-21	6.8	Microsoft Office Graphics Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31941. **CVE ID : CVE-2021-31940**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31940	A-MIC-365_-180621/247
N/A	08-Jun-21	6.8	Microsoft Office Graphics Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31940. **CVE ID : CVE-2021-31941**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31941	A-MIC-365_-180621/248
3d_viewer					
N/A	08-Jun-21	6.8	3D Viewer Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31943. **CVE ID : CVE-2021-31942**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31942	A-MIC-3D_V-180621/249
N/A	08-Jun-21	6.8	3D Viewer Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31942.	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-3D_V-180621/250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31943	guidance/advisory/CVE-2021-31943	
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	4.3	3D Viewer Information Disclosure Vulnerability **CVE ID : CVE-2021-31944**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31944	A-MIC-3D_V-180621/251
edge					
Improper Privilege Management	08-Jun-21	5.1	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability **CVE ID : CVE-2021-33741**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33741	A-MIC-EDGE-180621/252
excel					
N/A	08-Jun-21	6.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2021-31939**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31939	A-MIC-EXCE-180621/253
intune_management_extension					
N/A	08-Jun-21	7.5	Microsoft Intune Management Extension Remote Code Execution Vulnerability **CVE ID : CVE-2021-31980**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31980	A-MIC-INTU-180621/254
kubernetes_tools					
Improper Privilege Management	08-Jun-21	6.8	Microsoft VsCode Kubernetes Tools Extension Elevation of Privilege Vulnerability	https://portal.msrc.microsoft.com/en	A-MIC-KUBE-180621/255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31938	-US/security-guidance/advisory/CVE-2021-31938	
malware_protection_engine					
N/A	08-Jun-21	2.1	Microsoft Defender Denial of Service Vulnerability **CVE ID : CVE-2021-31978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31978	A-MIC-MALW-180621/256
N/A	08-Jun-21	6.8	Microsoft Defender Remote Code Execution Vulnerability **CVE ID : CVE-2021-31985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31985	A-MIC-MALW-180621/257
office					
N/A	08-Jun-21	6.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2021-31939**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31939	A-MIC-OFFI-180621/258
N/A	08-Jun-21	6.8	Microsoft Office Graphics Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31941. **CVE ID : CVE-2021-31940**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31940	A-MIC-OFFI-180621/259
N/A	08-Jun-21	6.8	Microsoft Office Graphics Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31940.	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	A-MIC-OFFI-180621/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31941	visory/CVE-2021-31941	
office_online_server					
N/A	08-Jun-21	6.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2021-31939**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31939	A-MIC-OFFI-180621/261
office_web_apps_server					
N/A	08-Jun-21	6.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2021-31939**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31939	A-MIC-OFFI-180621/262
outlook					
N/A	08-Jun-21	6.8	Microsoft Office Graphics Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31940. **CVE ID : CVE-2021-31941**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31941	A-MIC-OUTL-180621/263
paint_3d					
N/A	08-Jun-21	6.8	Paint 3D Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31946, CVE-2021-31983. **CVE ID : CVE-2021-31945**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31945	A-MIC-PAIN-180621/264
N/A	08-Jun-21	6.8	Paint 3D Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31945, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-PAIN-180621/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			31983. **CVE ID : CVE-2021-31946**	guidance/advisory/CVE-2021-31946	
N/A	08-Jun-21	6.8	Paint 3D Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31945, CVE-2021-31946. **CVE ID : CVE-2021-31983**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31983	A-MIC-PAIN-180621/266
sharepoint_enterprise_server					
N/A	08-Jun-21	6.5	Microsoft SharePoint Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31963, CVE-2021-31966. **CVE ID : CVE-2021-26420**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26420	A-MIC-SHAR-180621/267
sharepoint_foundation					
N/A	08-Jun-21	4	Microsoft SharePoint Server Information Disclosure Vulnerability **CVE ID : CVE-2021-31965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31965	A-MIC-SHAR-180621/268
N/A	08-Jun-21	6.5	Microsoft SharePoint Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26420, CVE-2021-31963. **CVE ID : CVE-2021-31966**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31966	A-MIC-SHAR-180621/269
N/A	08-Jun-21	6.5	Microsoft SharePoint Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31963, CVE-2021-31966.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	A-MIC-SHAR-180621/270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26420	2021-26420	
sharepoint_server					
N/A	08-Jun-21	4	Microsoft SharePoint Server Information Disclosure Vulnerability **CVE ID : CVE-2021-31965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31965	A-MIC-SHAR-180621/271
N/A	08-Jun-21	6.5	Microsoft SharePoint Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26420, CVE-2021-31963. **CVE ID : CVE-2021-31966**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31966	A-MIC-SHAR-180621/272
N/A	08-Jun-21	6.5	Microsoft SharePoint Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31963, CVE-2021-31966. **CVE ID : CVE-2021-26420**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26420	A-MIC-SHAR-180621/273
vp9_video_extensions					
N/A	08-Jun-21	6.8	VP9 Video Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2021-31967**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31967	A-MIC-VP9_-180621/274
mintty_project					
mintty					
Allocation of Resources Without Limits or Throttling	03-Jun-21	5	Mintty before 3.4.5 allows remote servers to cause a denial of service (Windows GUI hang) by telling the Mintty window to change its	https://github.com/mintty/mintty/commit/bd52109993440b6	A-MIN-MINT-180621/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			title repeatedly at high speed, which results in many SetWindowTextA or SetWindowTextW calls. In other words, it does not implement a usleep or similar delay upon processing a title change. **CVE ID : CVE-2021-28848**	996760aaccb66e68e782762b9, https://mintty.github.io/, https://github.com/mintty/mintty/compare/3.4.4...3.4.5	
Mobatek					
mobaxterm					
Uncontrolled Resource Consumption	03-Jun-21	5	MobaXterm before 21.0 allows remote servers to cause a denial of service (Windows GUI hang) via tab title change requests that are sent repeatedly at high speed, which results in many SetWindowTextA or SetWindowTextW calls. **CVE ID : CVE-2021-28847**	https://mobaxterm.mobatek.net/preview.html, https://mobaxterm.mobatek.net/download-home-edition.html	A-MOB-MOBA-180621/276
nestie_project					
nestie					
N/A	03-Jun-21	7.5	Prototype pollution vulnerability in 'nestie' versions 0.0.0 through 1.0.0 allows an attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2021-25947**	N/A	A-NES-NEST-180621/277
netlify					
kiali-operator					
Improper Preservation of	01-Jun-21	6.5	An incorrect access control flaw was found in the kiali-operator in versions before 1.33.0 and before 1.24.7. This	https://kiali.io/news/security-bulletins/kia	A-NET-KIAL-180621/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			flaw allows an attacker with a basic level of access to the cluster (to deploy a kiali operand) to use this vulnerability and deploy a given image to anywhere in the cluster, potentially gaining access to privileged service account tokens. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3495**	li-security-003/, https://bugzilla.redhat.com/show_bug.cgi?id=1947361	
Nextcloud					
nextcloud_mail					
Missing Authorization	01-Jun-21	4	Nextcloud Mail is a mail app for the Nextcloud platform. A missing permission check in Nextcloud Mail before 1.4.3 and 1.8.2 allows another authenticated users to access mail metadata of other users. Versions 1.4.3 and 1.8.2 contain patches for this vulnerability; no workarounds other than the patches are known to exist. **CVE ID : CVE-2021-32652**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-mxx2-6rg9-v2vc	A-NEX-NEXT-180621/279
nextcloud_server					
Insertion of Sensitive Information Into Sent Data	01-Jun-21	4	Nextcloud Server is a Nextcloud package that handles data storage. Nextcloud Server versions prior to 19.0.11, 20.0.10, or 21.0.2 send user IDs to the lookup server even if the user has no fields set to published. The vulnerability is patched	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-396j-vqpr-qg45	A-NEX-NEXT-180621/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in versions 19.0.11, 20.0.10, and 21.0.2; no workarounds outside the updates are known to exist. **CVE ID : CVE-2021-32653**		
Authorization Bypass Through User-Controlled Key	01-Jun-21	6.4	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.11, 20.0.10, and 21.0.2, an attacker is able to receive write/read privileges on any Federated File Share. Since public links can be added as federated file share, this can also be exploited on any public link. Users can upgrade to patched versions (19.0.11, 20.0.10 or 21.0.2) or, as a workaround, disable federated file sharing. **CVE ID : CVE-2021-32654**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-jf9h-v24c-22g5	A-NEX-NEXT-180621/281
N/A	01-Jun-21	3.5	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.11, 20.0.10, and 21.0.2, an attacker is able to convert a Files Drop link to a federated share. This causes an issue on the UI side of the sharing user. When the sharing user opens the sharing panel and tries to remove the "Create" privileges of this unexpected share, Nextcloud server would silently grant the share read privileges. The vulnerability is patched in versions 19.0.11, 20.0.10 and	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-grph-cm44-p3jv	A-NEX-NEXT-180621/282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			21.0.2. No workarounds are known to exist. **CVE ID : CVE-2021-32655**		
Improper Access Control	01-Jun-21	5	Nextcloud Server is a Nextcloud package that handles data storage. A vulnerability in federated share exists in versions prior to 19.0.11, 20.0.10, and 21.0.2. An attacker can gain access to basic information about users of a server by accessing a public link that a legitimate server user added as a federated share. This happens because Nextcloud supports sharing registered users with other Nextcloud servers, which can be done automatically when selecting the "Add server automatically once a federated share was created successfully" setting. The vulnerability is patched in versions 19.0.11, 20.0.10, and 21.0.2 As a workaround, disable "Add server automatically once a federated share was created successfully" in the Nextcloud settings. **CVE ID : CVE-2021-32656**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-j875-vr2q-h6x6	A-NEX-NEXT-180621/283
Uncontrolled Resource Consumption	01-Jun-21	4	Nextcloud Server is a Nextcloud package that handles data storage. In versions of Nextcloud Server prior to 10.0.11, 20.0.10, and 21.0.2, a malicious user may be able to break the user administration page. This	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-fx62-q47f-	A-NEX-NEXT-180621/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would disallow administrators to administrate users on the Nextcloud instance. The vulnerability is fixed in versions 19.0.11, 20.0.10, and 21.0.2. As a workaround, administrators can use the OCC command line tool to administrate the Nextcloud users. **CVE ID : CVE-2021-32657**	f665	
Nginx					
nginx					
Off-by-one Error	01-Jun-21	7.5	A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact. **CVE ID : CVE-2021-23017**	http://mailman.nginx.org/pipermail/nginx-announce/2021/000300.html	A-NGI-NGIN-180621/285
nitro_enclaves_project					
nitro_enclaves					
NULL Pointer Dereference	01-Jun-21	7.2	A flaw null pointer dereference in the Nitro Enclaves kernel driver was found in the way that Enclaves VMs forces closures on the enclave file descriptor. A local user of a host machine could use this flaw to crash the system or escalate their privileges on the system. **CVE ID : CVE-2021-3543**	N/A	A-NIT-NITR-180621/286
NSA					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
emissary					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-Jun-21	6.5	Emissary is a P2P based data-driven workflow engine. Affected versions of Emissary are vulnerable to post-authentication Remote Code Execution (RCE). The [`CreatePlace`](https://github.com/NationalSecurityAgency/emissary/blob/30c54ef16c6eb6ed09604a929939fb9f66868382/src/main/java/emissary/server/mvc/internal/CreatePlaceAction.java#L36) REST endpoint accepts an `sppClassName` parameter which is used to load an arbitrary class. This class is later instantiated using a constructor with the following signature: `<constructor>(String, String, String)`. An attacker may find a gadget (class) in the application classpath that could be used to achieve Remote Code Execution (RCE) or disrupt the application. Even though the chances to find a gadget (class) that allow arbitrary code execution are low, an attacker can still find gadgets that could potentially crash the application or leak sensitive data. As a work around disable network access to Emissary from untrusted sources. **CVE ID : CVE-2021-32647**	https://github.com/NationalSecurityAgency/emissary/security/advisories/GHSA-ph73-7v9r-wg32	A-NSA-EMIS-180621/287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Openexr					
openexr					
Out-of-bounds Write	08-Jun-21	6.8	A heap-buffer overflow was found in the copyIntoFrameBuffer function of OpenEXR in versions before 3.0.1. An attacker could use this flaw to execute arbitrary code with the permissions of the user running the application compiled against OpenEXR. **CVE ID : CVE-2021-23169**	N/A	A-OPE-OPEN-180621/288
Integer Overflow or Wraparound	08-Jun-21	4.3	An integer overflow leading to a heap-buffer overflow was found in the DwaCompressor of OpenEXR in versions before 3.0.1. An attacker could use this flaw to crash an application compiled with OpenEXR. **CVE ID : CVE-2021-23215**	N/A	A-OPE-OPEN-180621/289
Integer Underflow (Wrap or Wraparound)	08-Jun-21	4.3	An integer overflow leading to a heap-buffer overflow was found in the DwaCompressor of OpenEXR in versions before 3.0.1. An attacker could use this flaw to crash an application compiled with OpenEXR. This is a different flaw from CVE-2021-23215. **CVE ID : CVE-2021-26260**	N/A	A-OPE-OPEN-180621/290
Integer Underflow (Wrap or Wraparound)	08-Jun-21	4.3	An integer overflow leading to a heap-buffer overflow was found in OpenEXR in versions before 3.0.1. An attacker could use this flaw to crash an application compiled with	https://bugzilla.redhat.com/show_bug.cgi?id=1947591	A-OPE-OPEN-180621/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OpenEXR. **CVE ID : CVE-2021-26945**		
Opennms					
meridian					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to Stored Cross-Site Scripting, since the function `validateFormInput()` performs improper validation checks on the input sent to the `userID` parameter. Due to this flaw an attacker could inject an arbitrary script which will be stored in the database. **CVE ID : CVE-2021-25932**	https://github.com/OpenNMS/opennms/commit/f3ebfa3da5352b4d57f238b54c6db315ad99f10e, https://github.com/OpenNMS/opennms/commit/eb08b5ed4c5548f3e941a1f0d0363ae4439fa98c, https://github.com/OpenNMS/opennms/commit/8a97e6869d6e49da18b208c837438ace80049c01	A-OPE-MERI-180621/292
opennms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are	https://github.com/OpenNMS/opennms/commit/f3ebfa3da5352b4d57f238b54c6db315ad99f10e, https://github.com/Open	A-OPE-OPEN-180621/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to Stored Cross-Site Scripting, since the function `validateFormInput()` performs improper validation checks on the input sent to the `userID` parameter. Due to this flaw an attacker could inject an arbitrary script which will be stored in the database. **CVE ID : CVE-2021-25932**	NMS/opennms/commit/eb08b5ed4c5548f3e941a1f0d0363ae4439fa98c, https://github.com/OpenNMS/opennms/commit/8a97e6869d6e49da18b208c837438ace80049c01	
ovn					
ovn-kubernetes					
Incorrect Authorization	02-Jun-21	7.5	A vulnerability was found in OVN Kubernetes in versions up to and including 0.3.0 where the Egress Firewall does not reliably apply firewall rules when there is multiple DNS rules. It could lead to potentially lose of confidentiality, integrity or availability of a service. **CVE ID : CVE-2021-3499**	N/A	A-OVN-OVN--180621/294
Postgresql					
postgresql					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jun-21	6.5	A flaw was found in postgresql in versions before 13.3, before 12.7, before 11.12, before 10.17 and before 9.6.22. While modifying certain SQL array values, missing bounds checks let authenticated database users write arbitrary bytes to a wide area	https://www.postgresql.org/support/security/CVE-2021-32027/, https://bugzilla.redhat.com/show_bug.cgi?id=1956	A-POS-POST-180621/295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of server memory. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-32027**	876	
purethemes					
listeo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	The Listeo WordPress theme before 1.6.11 did not properly sanitise some parameters in its Search, Booking Confirmation and Personal Message pages, leading to Cross-Site Scripting issues **CVE ID : CVE-2021-24317**	https://wpscan.com/vulnerability/704d8886-df9e-4217-88d1-a72a71924174	A-PUR-LIST-180621/296
Improper Access Control	01-Jun-21	5.5	The Listeo WordPress theme before 1.6.11 did not ensure that the Post/Page and Booking to delete belong to the user making the request, allowing any authenticated users to delete arbitrary page/post and booking via an IDOR vector. **CVE ID : CVE-2021-24318**	https://wpscan.com/vulnerability/9afa7e11-68b3-4196-975e-8b3f8e68ce56	A-PUR-LIST-180621/297
Python					
pillow					
Out-of-bounds Read	02-Jun-21	6.4	An issue was discovered in Pillow before 8.2.0. There is an out-of-bounds read in J2kDecode, in j2ku_graya_la. **CVE ID : CVE-2021-25287**	https://pillow.readthedocs.io/en/stable/releasenotes/8.2.0.html#cve-2021-25287-cve-2021-25288-fix-oob-read-	A-PYT-PILL-180621/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				in-jpeg2kdecode	
Out-of-bounds Read	02-Jun-21	6.4	An issue was discovered in Pillow before 8.2.0. There is an out-of-bounds read in J2kDecode, in j2ku_gray_i. **CVE ID : CVE-2021-25288**	https://pillow.readthedocs.io/en/stable/releasenotes/8.2.0.html#cve-2021-25287-cve-2021-25288-fix-oob-read-in-jpeg2kdecode	A-PYT-PILL-180621/299
Unchecked Return Value	02-Jun-21	4.3	An issue was discovered in Pillow before 8.2.0. PSDImagePlugin.PsdImageFile lacked a sanity check on the number of input layers relative to the size of the data block. This could lead to a DoS on Image.open prior to Image.load. **CVE ID : CVE-2021-28675**	https://pillow.readthedocs.io/en/stable/releasenotes/8.2.0.html#cve-2021-28675-fix-dos-in-psdimageplugin	A-PYT-PILL-180621/300
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jun-21	5	An issue was discovered in Pillow before 8.2.0. For FLI data, FliDecode did not properly check that the block advance was non-zero, potentially leading to an infinite loop on load. **CVE ID : CVE-2021-28676**	N/A	A-PYT-PILL-180621/301
N/A	02-Jun-21	5	An issue was discovered in Pillow before 8.2.0. For EPS data, the readline implementation used in EPSImageFile has to deal with any combination of \r	https://github.com/python-pillow/Pillow/pull/5377	A-PYT-PILL-180621/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and \n as line endings. It used an accidentally quadratic method of accumulating lines while looking for a line ending. A malicious EPS file could use this to perform a DoS of Pillow in the open phase, before an image was accepted for opening. **CVE ID : CVE-2021-28677**		
Insufficient Verification of Data Authenticity	02-Jun-21	4.3	An issue was discovered in Pillow before 8.2.0. For BLP data, BlpImagePlugin did not properly check that reads (after jumping to file offsets) returned data. This could lead to a DoS where the decoder could be run a large number of times on empty data. **CVE ID : CVE-2021-28678**	https://github.com/python-pillow/Pillow/pull/5377, https://pillow.readthedocs.io/en/stable/releasenotes/8.2.0.html#cve-2021-28678-fix-blp-dos	A-PYT-PILL-180621/303
Qemu					
qemu					
Missing Release of Memory after Effective Lifetime	02-Jun-21	2.1	Several memory leaks were found in the virtio vhost-user GPU device (vhost-user-gpu) of QEMU in versions up to and including 6.0. They exist in contrib/vhost-user-gpu/vhost-user-gpu.c and contrib/vhost-user-gpu/virgl.c due to improper release of memory (i.e., free) after effective lifetime. **CVE ID : CVE-2021-3544**	N/A	A-QEM-QEMU-180621/304
Exposure of	02-Jun-21	2.1	An information disclosure	N/A	A-QEM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information to an Unauthorized Actor			vulnerability was found in the virtio vhost-user GPU device (vhost-user-gpu) of QEMU in versions up to and including 6.0. The flaw exists in virgl_cmd_get_capset_info() in contrib/vhost-user-gpu/virgl.c and could occur due to the read of uninitialized memory. A malicious guest could exploit this issue to leak memory from the host. **CVE ID : CVE-2021-3545**		QEMU-180621/305
Out-of-bounds Write	02-Jun-21	4.6	A flaw was found in vhost-user-gpu of QEMU in versions up to and including 6.0. An out-of-bounds write vulnerability can allow a malicious guest to crash the QEMU process on the host resulting in a denial of service or potentially execute arbitrary code on the host with the privileges of the QEMU process. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3546**	N/A	A-QEM-QEMU-180621/306
Qnap					
q\\"center					
Improper Neutralization of Input During Web Page Generation	03-Jun-21	3.5	A post-authentication reflected XSS vulnerability has been reported to affect QNAP NAS running Q'center. If exploited, this vulnerability allows remote attackers to	https://www.qnap.com/zh-tw/security-advisory/qsa-21-20	A-QNA-Q\\'-180621/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			inject malicious code. QNAP have already fixed this vulnerability in the following versions of Q'center: QTS 4.5.3: Q'center v1.12.1012 and later QTS 4.3.6: Q'center v1.10.1004 and later QTS 4.3.3: Q'center v1.10.1004 and later QuTS hero h4.5.2: Q'center v1.12.1012 and later QuTScloud c4.5.4: Q'center v1.12.1012 and later **CVE ID : CVE-2021-28807**		
video_station					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Jun-21	6.5	A command injection vulnerability has been reported to affect certain versions of Video Station. If exploited, this vulnerability allows remote attackers to execute arbitrary commands. This issue affects: QNAP Systems Inc. Video Station versions prior to 5.5.4 on QTS 4.5.2; versions prior to 5.5.4 on QuTS hero h4.5.2; versions prior to 5.5.4 on QuTScloud c4.5.4. This issue does not affect: QNAP Systems Inc. Video Station on QTS 4.3.6; on QTS 4.3.3. **CVE ID : CVE-2021-28812**	https://www.qnap.com/zh-tw/security-advisory/qsa-21-21	A-QNA-VIDE-180621/308
Redhat					
3scale					
Improper Restriction of Excessive Authentication Attempts	01-Jun-21	5	It was found that all versions of 3Scale developer portal lacked brute force protections. An attacker could use this gap to bypass	https://bugzilla.redhat.com/show_bug.cgi?id=1928301	A-RED-3SCA-180621/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			login controls, and access privileged information, or possibly conduct further attacks. **CVE ID : CVE-2021-3412**		
3scale_api_management					
Improper Restriction of Excessive Authentication Attempts	01-Jun-21	5	It was found that all versions of 3Scale developer portal lacked brute force protections. An attacker could use this gap to bypass login controls, and access privileged information, or possibly conduct further attacks. **CVE ID : CVE-2021-3412**	https://bugzilla.redhat.com/show_bug.cgi?id=1928301	A-RED-3SCA-180621/310
descision_manager					
Incorrect Authorization	01-Jun-21	4	A flaw was found in the BPMN editor in version jBPM 7.51.0.Final. Any authenticated user from any project can see the name of Ruleflow Groups from other projects, despite the user not having access to those projects. The highest threat from this vulnerability is to confidentiality. **CVE ID : CVE-2021-20306**	https://bugzilla.redhat.com/show_bug.cgi?id=1946213	A-RED-DESC-180621/311
jboss_a-mq					
Insertion of Sensitive Information into Log File	01-Jun-21	2.1	A flaw was found in the AMQ Broker that discloses JDBC encrypted usernames and passwords when provided in the AMQ Broker application logfile when using the jdbc persistence functionality. Versions shipped in Red Hat	https://bugzilla.redhat.com/show_bug.cgi?id=1936629	A-RED-JBOS-180621/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AMQ 7 are vulnerable. **CVE ID : CVE-2021-3425**		
jboss_core_services					
Use After Free	01-Jun-21	6.8	There's a flaw in libxml2's xmllint in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by xmllint could trigger a use-after-free. The greatest impact of this flaw is to confidentiality, integrity, and availability. **CVE ID : CVE-2021-3516**	https://gitlab.gnome.org/GNOME/libxml2/-/commit/1358d157d0bd83be1dfe356a69213df9fac0b539	A-RED-JBOS-180621/313
jboss_enterprise_application_platform					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jun-21	6.5	A flaw was found in postgresql in versions before 13.3, before 12.7, before 11.12, before 10.17 and before 9.6.22. While modifying certain SQL array values, missing bounds checks let authenticated database users write arbitrary bytes to a wide area of server memory. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-32027**	https://www.postgresql.org/support/security/CVE-2021-32027/, https://bugzilla.redhat.com/show_bug.cgi?id=1956876	A-RED-JBOS-180621/314
jbpm					
Incorrect Authorization	01-Jun-21	4	A flaw was found in the BPMN editor in version jBPM 7.51.0.Final. Any authenticated user from any project can see the name of Ruleflow Groups from other projects, despite the user not	https://bugzilla.redhat.com/show_bug.cgi?id=1946213	A-RED-JBPM-180621/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			having access to those projects. The highest threat from this vulnerability is to confidentiality. **CVE ID : CVE-2021-20306**		
noobaa-operator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	6.8	A flaw was found in noobaa-core in versions before 5.7.0. This flaw results in the name of an arbitrarily URL being copied into an HTML document as plain text between tags, including potentially a payload script. The input was echoed unmodified in the application response, resulting in arbitrary JavaScript being injected into an application's response. The highest threat to the system is for confidentiality, availability, and integrity. **CVE ID : CVE-2021-3529**	N/A	A-RED-NOOB-180621/316
openshift_container_platform					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-21	6.8	A flaw was found in noobaa-core in versions before 5.7.0. This flaw results in the name of an arbitrarily URL being copied into an HTML document as plain text between tags, including potentially a payload script. The input was echoed unmodified in the application response, resulting in arbitrary JavaScript being injected into an application's response. The highest threat	N/A	A-RED-OPEN-180621/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the system is for confidentiality, availability, and integrity. **CVE ID : CVE-2021-3529**		
openshift_service_mesh					
Improper Preservation of Permissions	01-Jun-21	6.5	An incorrect access control flaw was found in the kiali-operator in versions before 1.33.0 and before 1.24.7. This flaw allows an attacker with a basic level of access to the cluster (to deploy a kiali operand) to use this vulnerability and deploy a given image to anywhere in the cluster, potentially gaining access to privileged service account tokens. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3495**	https://kiali.io/news/security-bulletins/kiali-security-003/, https://bugzilla.redhat.com/show_bug.cgi?id=1947361	A-RED-OPEN-180621/318
process_automation					
Incorrect Authorization	01-Jun-21	4	A flaw was found in the BPMN editor in version jBPM 7.51.0.Final. Any authenticated user from any project can see the name of Ruleflow Groups from other projects, despite the user not having access to those projects. The highest threat from this vulnerability is to confidentiality. **CVE ID : CVE-2021-20306**	https://bugzilla.redhat.com/show_bug.cgi?id=1946213	A-RED-PROC-180621/319
single_sign-on					
Improper	01-Jun-21	5	A flaw was found in keycloak	https://bugz	A-RED-SING-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			as shipped in Red Hat Single Sign-On 7.4 where IDN homograph attacks are possible. A malicious user can register himself with a name already registered and trick admin to grant him extra privileges. **CVE ID : CVE-2021-3424**	illa.redhat.com/show_bug.cgi?id=1933320	180621/320
software_collections					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jun-21	6.5	A flaw was found in postgresql in versions before 13.3, before 12.7, before 11.12, before 10.17 and before 9.6.22. While modifying certain SQL array values, missing bounds checks let authenticated database users write arbitrary bytes to a wide area of server memory. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-32027**	https://www.postgresql.org/support/security/CVE-2021-32027/, https://bugzilla.redhat.com/show_bug.cgi?id=1956876	A-RED-SOFT-180621/321
redislabs					
redis					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jun-21	6.5	Redis is an open source (BSD licensed), in-memory data structure store, used as a database, cache, and message broker. An integer overflow bug in Redis version 6.0 or newer (on 32-bit systems ONLY) can be exploited using the `STRALGO LCS` command to corrupt the heap and potentially result with	https://github.com/redis/redis/security/advisories/GHSA-46cp-x4x9-6pfq	A-RED-REDI-180621/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote code execution. This is a result of an incomplete fix for CVE-2021-29477 which only addresses the problem on 64-bit systems but fails to do that for 32-bit. 64-bit systems are not affected. The problem is fixed in version 6.2.4 and 6.0.14. An additional workaround to mitigate the problem without patching the `redis-server` executable is to use ACL configuration to prevent clients from using the `STRALGO LCS` command. **CVE ID : CVE-2021-32625**		
refined-github_project					
refined-github					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-21	4.3	The Refined GitHub browser extension before 21.6.8 might allow XSS via a link in a document. NOTE: github.com sends Content-Security-Policy headers to, in general, address XSS and other concerns. **CVE ID : CVE-2021-34364**	N/A	A-REF-REFI-180621/323
SAP					
3d_visual_enterprise_viewer					
Improper Input Validation	09-Jun-21	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated GIF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this	https://launchpad.support.sap.com/#/notes/3059999, https://wiki.scn.sap.com/wiki/pages/viewpage.act	A-SAP-3D_V-180621/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is caused due to Improper Input Validation. **CVE ID : CVE-2021-33659**	ion?pageId=578125999	
Improper Input Validation	09-Jun-21	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated FLI file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2021-33660**	https://launchpad.support.sap.com/#/notes/3059999, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-3D_V-180621/325
Improper Input Validation	09-Jun-21	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2021-33661**	https://launchpad.support.sap.com/#/notes/3059999, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-3D_V-180621/326
Improper Input Validation	09-Jun-21	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated JT file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2021-27638**	https://launchpad.support.sap.com/#/notes/3059999, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-3D_V-180621/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-Jun-21	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated JT file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2021-27639**	https://launchpad.support.sap.com/#/notes/3059999, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-3D_V-180621/328
Improper Input Validation	09-Jun-21	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PSD file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2021-27640**	https://launchpad.support.sap.com/#/notes/3059999, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-3D_V-180621/329
Improper Input Validation	09-Jun-21	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated TIF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2021-27641**	https://launchpad.support.sap.com/#/notes/3059999, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-3D_V-180621/330
Improper Input Validation	09-Jun-21	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated	https://launchpad.support.sap.com/#	A-SAP-3D_V-180621/331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2021-27642**	/notes/3059999, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	
Improper Input Validation	09-Jun-21	4.3	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated IFF file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation. **CVE ID : CVE-2021-27643**	https://launchpad.support.sap.com/#/notes/3059999, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-3D_V-180621/332
netweaver_abap					
Improper Input Validation	09-Jun-21	5	SAP NetWeaver AS for ABAP (RFC Gateway), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77, 7.81,7.82,7.83, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method memmove() causing	https://launchpad.support.sap.com/#/notes/3020209, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-180621/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27597**		
Improper Input Validation	09-Jun-21	5	SAP NetWeaver AS for ABAP (RFC Gateway), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77, 7.81,7.82,7.83, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method ThCPIC() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27633**	https://launchpad.support.sap.com/#/notes/3020209, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-180621/334
Improper Input Validation	09-Jun-21	4.3	SAP NetWeaver AS for ABAP (RFC Gateway), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77, 7.81,7.82,7.83, allows an	https://launchpad.support.sap.com/#/notes/3020209, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=	A-SAP-NETW-180621/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method ThCpicDtCreate () causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27634**	578125999	
netweaver_as_abap					
Improper Input Validation	09-Jun-21	5	SAP NetWeaver ABAP Server and ABAP Platform (Enqueue Server), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method EncOAMParamStore() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.	https://launchpad.support.sap.com/#/notes/3020104, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-180621/336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-27606		
Improper Input Validation	09-Jun-21	5	SAP NetWeaver ABAP Server and ABAP Platform (Enqueue Server), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method EncPSetUnsupported() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27629**	https://launchpad.support.sap.com/#/notes/3020104, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-180621/337
Improper Input Validation	09-Jun-21	5	SAP NetWeaver ABAP Server and ABAP Platform (Enqueue Server), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73, allows an unauthenticated attacker without specific knowledge of the system to	https://launchpad.support.sap.com/#/notes/3020104, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-180621/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method EnqConvUniToSrvReq() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27630**		
Improper Input Validation	09-Jun-21	5	SAP NetWeaver ABAP Server and ABAP Platform (Enqueue Server), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method EnqConvUniToSrvReq() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27631**	https://launchpad.support.sap.com/#/notes/3020104, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-180621/339
Improper	09-Jun-21	5	SAP NetWeaver ABAP Server	https://laun	A-SAP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			and ABAP Platform (Enqueue Server), versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73, allows an unauthenticated attacker without specific knowledge of the system to send a specially crafted packet over a network which will trigger an internal error in the system due to improper input validation in method EnqConvUniToSrvReq() causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27632**	chpad.support.sap.com/#/notes/3020104, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	NETW-180621/340
netweaver_as_internet_graphics_server					
Improper Input Validation	09-Jun-21	4.3	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method Ups::AddPart() which will trigger an internal memory corruption error in the system causing the	https://launchpad.support.sap.com/#/notes/3021050, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-180621/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27620**		
Improper Input Validation	09-Jun-21	4.3	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method CDrawRaster::LoadImageFromMemory() which will trigger an internal memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27622**	https://launchpad.support.sap.com/#/notes/3021050, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-180621/342
Improper Input Validation	09-Jun-21	4.3	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method CXmlUtility::CheckLength() which will trigger an internal	https://launchpad.support.sap.com/#/notes/3021050, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-180621/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27623**		
Improper Input Validation	09-Jun-21	4.3	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method CiXMLIStreamRawBuffer::readRaw () which will trigger an internal memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27624**	https://launchpad.support.sap.com/#/notes/3021050, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-180621/344
Improper Input Validation	09-Jun-21	4.3	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method	https://launchpad.support.sap.com/#/notes/3021050, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-180621/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IgsData::freeMemory() which will trigger an internal memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27625**		
Improper Input Validation	09-Jun-21	5	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method CMiniXMLParser::Parse() which will trigger an internal memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27626**	https://launchpad.support.sap.com/#/notes/3021050, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-180621/346
Improper Input Validation	09-Jun-21	4.3	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to	https://launchpad.support.sap.com/#/notes/3021050, https://wiki.scn.sap.com/wiki/pages/viewpage.act	A-SAP-NETW-180621/347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation in method ChartInterpreter::DoIt() which will trigger an internal memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified. **CVE ID : CVE-2021-27627**	ion?pageId=578125999	
smartdatasoft					
car_repair_services_\\&_auto_mechanic					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	The Car Repair Services & Auto Mechanic WordPress theme before 4.0 did not properly sanitise its serviceestimatekey search parameter before outputting it back in the page, leading to a reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24335**	https://wpscan.com/vulnerability/39258aba-2449-4214-a490-b8e46945117d	A-SMA-CAR_-180621/348
smooth_scroll_page_up\\/down_buttons_project					
Synology					
diskstation_manager					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Jun-21	4.6	Improper limitation of a pathname to a restricted directory ('Path Traversal') in cgi component in Synology DiskStation Manager (DSM) before 6.2.4-25553 allows local users to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2021-29088**	https://www.synology.com/security/advisory/Synology_SA_21_03	A-SYN-DISK-180621/349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Jun-21	4	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in PDF Viewer component in Synology DiskStation Manager (DSM) before 6.2.4-25553 allows remote authenticated users to read limited files via unspecified vectors. **CVE ID : CVE-2021-33182**	https://www.synology.com/security/advisory/Synology_SA_21_03	A-SYN-DISK-180621/350
docker					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Jun-21	3.6	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability container volume management component in Synology Docker before 18.09.0-0515 allows local users to read or write arbitrary files via unspecified vectors. **CVE ID : CVE-2021-33183**	https://www.synology.com/security/advisory/Synology_SA_21_08	A-SYN-DOCK-180621/351
download_station					
Server-Side Request Forgery (SSRF)	01-Jun-21	4	Server-Side request forgery (SSRF) vulnerability in task management component in Synology Download Station before 3.8.15-3563 allows remote authenticated users to read arbitrary files via unspecified vectors. **CVE ID : CVE-2021-33184**	https://www.synology.com/security/advisory/Synology_SA_20_23	A-SYN-DOWN-180621/352
media_server					
Improper Neutralization of Special Elements	01-Jun-21	7.5	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in cgi	https://www.synology.com/security/advisory/Sy	A-SYN-MEDI-180621/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			component in Synology Media Server before 1.8.1-2876 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. **CVE ID : CVE-2021-33180**	nology_SA_20_24	
photo_station					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-21	10	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in thumbnail component in Synology Photo Station before 6.8.14-3500 allows remote attackers users to execute arbitrary SQL commands via unspecified vectors. **CVE ID : CVE-2021-29089**	https://www.synology.com/security/advisory/Synology_SA_20_20	A-SYN-PHOT-180621/354
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-21	9	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in PHP component in Synology Photo Station before 6.8.14-3500 allows remote authenticated users to execute arbitrary SQL command via unspecified vectors. **CVE ID : CVE-2021-29090**	https://www.synology.com/security/advisory/Synology_SA_20_20	A-SYN-PHOT-180621/355
Improper Limitation of a Pathname to a Restricted Directory ('Path	02-Jun-21	4	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in file management component in Synology Photo Station before 6.8.14-3500 allows	https://www.synology.com/security/advisory/Synology_SA_20_20	A-SYN-PHOT-180621/356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			remote authenticated users to write arbitrary files via unspecified vectors. **CVE ID : CVE-2021-29091**		
Unrestricted Upload of File with Dangerous Type	01-Jun-21	6.5	Unrestricted upload of file with dangerous type vulnerability in file management component in Synology Photo Station before 6.8.14-3500 allows remote authenticated users to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2021-29092**	https://www.synology.com/security/advisory/Synology_SA_20_20	A-SYN-PHOT-180621/357
video_station					
Server-Side Request Forgery (SSRF)	01-Jun-21	6.5	Server-Side Request Forgery (SSRF) vulnerability in webapi component in Synology Video Station before 2.4.10-1632 allows remote authenticated users to send arbitrary request to intranet resources via unspecified vectors. **CVE ID : CVE-2021-33181**	https://www.synology.com/security/advisory/Synology_SA_21_04	A-SYN-VIDE-180621/358
Theforeman					
foreman					
Incorrect Authorization	03-Jun-21	3.5	Foreman versions before 2.3.4 and before 2.4.0 is affected by an improper authorization handling flaw. An authenticated attacker can impersonate the foreman-proxy if product enable the Puppet Certificate authority (CA) to sign certificate requests that have subject alternative names (SANs).	N/A	A-THE-FORE-180621/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Foreman do not enable SANs by default and `allow-authorization-extensions` is set to `false` unless user change `/etc/puppetlabs/puppetserver/conf.d/ca.conf` configuration explicitly. **CVE ID : CVE-2021-3469**		
tpm2-tools_project					
tpm2-tools					
Exposure of Sensitive Information to an Unauthorized Actor	04-Jun-21	4.3	A flaw was found in tpm2-tools in versions before 5.1.1 and before 4.3.2. tpm2_import used a fixed AES key for the inner wrapper, potentially allowing a MITM attacker to unwrap the inner portion and reveal the key being imported. The highest threat from this vulnerability is to data confidentiality. **CVE ID : CVE-2021-3565**	https://bugzilla.redhat.com/show_bug.cgi?id=1964427	A-TPM-TPM2-180621/360
vembu					
bdr_suite					
N/A	08-Jun-21	7.5	Vembu BDR Suite before 4.2.0 allows Unauthenticated Remote Code Execution by placing a command in a GET request (issue 1 of 2). **CVE ID : CVE-2021-26471**	N/A	A-VEM-BDR_-180621/361
N/A	08-Jun-21	7.5	Vembu BDR Suite before 4.2.0 allows Unauthenticated Remote Code Execution by placing a command in a GET request (issue 2 of 2). **CVE ID : CVE-2021-26472**	N/A	A-VEM-BDR_-180621/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	08-Jun-21	7.5	Vembu BDR Suite before 4.2.0 allows Unauthenticated file write via a GET request that specifies a file's name and content. **CVE ID : CVE-2021-26473**	N/A	A-VEM-BDR_-180621/363
Server-Side Request Forgery (SSRF)	08-Jun-21	5	Vembu BDR Suite before 4.2.0 allows Unauthenticated SSRF via a GET request that specifies a hostname and port number. **CVE ID : CVE-2021-26474**	N/A	A-VEM-BDR_-180621/364
offsite_dr					
N/A	08-Jun-21	7.5	Vembu BDR Suite before 4.2.0 allows Unauthenticated Remote Code Execution by placing a command in a GET request (issue 1 of 2). **CVE ID : CVE-2021-26471**	N/A	A-VEM-OFFS-180621/365
N/A	08-Jun-21	7.5	Vembu BDR Suite before 4.2.0 allows Unauthenticated Remote Code Execution by placing a command in a GET request (issue 2 of 2). **CVE ID : CVE-2021-26472**	N/A	A-VEM-OFFS-180621/366
Unrestricted Upload of File with Dangerous Type	08-Jun-21	7.5	Vembu BDR Suite before 4.2.0 allows Unauthenticated file write via a GET request that specifies a file's name and content. **CVE ID : CVE-2021-26473**	N/A	A-VEM-OFFS-180621/367
Server-Side Request Forgery (SSRF)	08-Jun-21	5	Vembu BDR Suite before 4.2.0 allows Unauthenticated SSRF via a GET request that specifies a hostname and port number. **CVE ID : CVE-2021-26474**	N/A	A-VEM-OFFS-180621/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
veronalabs					
wp_statistics					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jun-21	5	The WP Statistics WordPress plugin before 13.0.8 relied on using the WordPress esc_sql() function on a field not delimited by quotes and did not first prepare the query. Additionally, the page, which should have been accessible to administrator only, was also available to any visitor, including unauthenticated ones. **CVE ID : CVE-2021-24340**	https://wpscan.com/vulnerability/d2970cfb-0aa9-4516-9a4b-32971f41a19c	A-VER-WP_S-180621/369
video_embed_project					
video_embed					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jun-21	6.5	The id GET parameter of one of the Video Embed WordPress plugin through 1.0's page (available via forced browsing) is not sanitised, validated or escaped before being used in a SQL statement, allowing low privilege users, such as subscribers, to perform SQL injection. **CVE ID : CVE-2021-24337**	https://wpscan.com/vulnerability/a8fd8dd4-5b5e-462e-8dae-065d5e2d003a	A-VID-VIDE-180621/370
weekly_schedule_project					
weekly_schedule					
Improper Neutralization of Input During Web Page Generation ('Cross-site	01-Jun-21	3.5	The "Schedule Name" input in the Weekly Schedule WordPress plugin before 3.4.3 general options did not properly sanitize input, allowing a user to inject javascript code using the	https://wpscan.com/vulnerability/ba1d01dc-16e4-464f-94be-ed311ff6ccf9	A-WEE-WEEK-180621/371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			<script> HTML tags and cause a stored XSS issue **CVE ID : CVE-2021-24309**		
wire					
wire					
Insufficient Verification of Data Authenticity	03-Jun-21	5	wire-ios is the iOS version of Wire, an open-source secure messaging app. wire-ios versions 3.8.0 and earlier have a bug in which a conversation could be incorrectly set to "unverified. This occurs when: - Self user is added to a new conversation - Self user is added to an existing conversation - All the participants in the conversation were previously marked as verified. The vulnerability is patched in wire-ios version 3.8.1. As a workaround, one can unverify & verify a device in the conversation. **CVE ID : CVE-2021-32665**	https://github.com/wireapp/wire-ios-data-model/commit/bf9db85886b12a20c8374f55b7c4a610e8ae9220, https://github.com/wireapp/wire-ios/security/advisories/GHSA-mc65-7w99-c6qv	A-WIR-WIRE-180621/372
Improper Input Validation	03-Jun-21	4	wire-ios is the iOS version of Wire, an open-source secure messaging app. In wire-ios versions 3.8.0 and prior, a vulnerability exists that can cause a denial of service between users. If a user has an invalid assetID for their profile picture and it contains the " character, it will cause the iOS client to crash. The vulnerability is patched in wire-ios version 3.8.1.	https://github.com/wireapp/wire-ios/security/advisories/GHSA-2x9x-vh27-h4rv, https://github.com/wireapp/wire-ios-data-model/commit/35af3f6	A-WIR-WIRE-180621/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-32666	32085f51a2ce7f608fdaeffd1a69ad89f	
Wireshark					
wireshark					
Loop with Unreachable Exit Condition ('Infinite Loop')	07-Jun-21	5	Infinite loop in DVB-S2-BB dissector in Wireshark 3.4.0 to 3.4.5 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2021-22222**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22222.json, https://www.wireshark.org/security/wnpa-sec-2021-05.html, https://gitlab.com/wireshark/wireshark/-/merge_requests/3130	A-WIR-WIRE-180621/374
wowthemes					
mediumish					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	The search feature of the Mediumish WordPress theme through 1.0.47 does not properly sanitise it's 's' GET parameter before output it back the page, leading to the Cross-SIte Scripting issue. **CVE ID : CVE-2021-24316**	https://www.wowthemes.net/themes/mediumish-wordpress/, https://wpscan.com/vulnerability/57e27de4-58f5-46aa-9b59-809705733b2e	A-WOW-MEDI-180621/375
Xmlsoft					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xmllint					
Use After Free	01-Jun-21	6.8	There's a flaw in libxml2's xmllint in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by xmllint could trigger a use-after-free. The greatest impact of this flaw is to confidentiality, integrity, and availability. **CVE ID : CVE-2021-3516**	https://gitlab.gnome.org/GNOME/libxml2/-/commit/1358d157d0bd83be1dfe356a69213df9fac0b539	A-XML-XMLL-180621/376
zavedil					
flightlog					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jun-21	6.5	The FlightLog WordPress plugin through 3.0.2 does not sanitise, validate or escape various POST parameters before using them a SQL statement, leading to SQL injections exploitable by editor and administrator users **CVE ID : CVE-2021-24336**	https://wpscan.com/vulnerability/dda0593e-cd97-454e-a8c8-15d7f690311c	A-ZAV-FLIG-180621/377
Zohocorp					
manageengine_key_manager_plus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-21	3.5	Zoho ManageEngine Key Manager Plus before 6001 allows Stored XSS on the user-management page while importing malicious user details from AD. **CVE ID : CVE-2021-28382**	https://www.manageengine.com/key-manager/release-notes.html#6001	A-ZOH-MANA-180621/378
Hardware					
chiyu-tech					
bf-430					
N/A	04-Jun-21	6.4	A CRLF injection vulnerability	https://ww	H-CHI-BF-4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			was found on BF-430, BF-431, and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of validation on the parameter redirect= available on multiple CGI components. **CVE ID : CVE-2021-31249**	w.chiyu-tech.com/msg/message-Firmware-update-87.html	180621/379
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-21	3.5	Multiple storage XSS vulnerabilities were discovered on BF-430, BF-431 and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of sanitization of the input on the components man.cgi, if.cgi, dhcpc.cgi, ppp.cgi. **CVE ID : CVE-2021-31250**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.htm	H-CHI-BF-4-180621/380
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-4-180621/381
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices	https://www.chiyu-tech.com/msg/message-Firmware-	H-CHI-BF-4-180621/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	update-87.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-4-180621/383
bf-431					
N/A	04-Jun-21	6.4	A CRLF injection vulnerability was found on BF-430, BF-431, and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of validation on the parameter redirect= available on multiple CGI components. **CVE ID : CVE-2021-31249**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-4-180621/384
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-21	3.5	Multiple storage XSS vulnerabilities were discovered on BF-430, BF-431 and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of sanitization of the input on the components man.cgi, if.cgi, dhcpc.cgi, ppp.cgi. **CVE ID : CVE-2021-31250**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.htm	H-CHI-BF-4-180621/385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-4-180621/386
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-4-180621/387
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-4-180621/388
bf-450m					
N/A	04-Jun-21	6.4	A CRLF injection vulnerability	https://ww	H-CHI-BF-4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			was found on BF-430, BF-431, and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of validation on the parameter redirect= available on multiple CGI components. **CVE ID : CVE-2021-31249**	w.chiyu-tech.com/msg/message-Firmware-update-87.html	180621/389
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-21	3.5	Multiple storage XSS vulnerabilities were discovered on BF-430, BF-431 and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of sanitization of the input on the components man.cgi, if.cgi, dhcpc.cgi, ppp.cgi. **CVE ID : CVE-2021-31250**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.htm	H-CHI-BF-4-180621/390
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-4-180621/391
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices	https://www.chiyu-tech.com/msg/message-Firmware-	H-CHI-BF-4-180621/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	update-87.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-4-180621/393
bf-630					
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-6-180621/394
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated.	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-6-180621/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31641		
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-6-180621/396
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-6-180621/397
bf-631					
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-6-180621/398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reboot of the device. **CVE ID : CVE-2021-31642**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-6-180621/399
bf-631w					
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-6-180621/400
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-6-180621/401
bf-830w					
URL Redirection to Untrusted	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431,	https://www.chiyu-tech.com/ms	H-CHI-BF-8-180621/402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	g/message-Firmware-update-87.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BF-8-180621/403
bfminiw					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BFMI-180621/404
biosense					
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The	https://www.chiyu-tech.com/msg/message-Firmware-update-	H-CHI-BIOS-180621/405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	87.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-BIOS-180621/406
semac_d1					
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/407
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that	https://www.chiyu-tech.com/msg/message-Firmware-update-	H-CHI-SEMA-180621/408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	87.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/409
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/410
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter.	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31643		
semac_d2					
Improper Authenticati on	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://ww w.chiyu-tech.com/ms g/message-Firmware-update-87.html	H-CHI-SEMA-180621/412
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://ww w.chiyu-tech.com/ms g/message-Firmware-update-87.html	H-CHI-SEMA-180621/413
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://ww w.chiyu-tech.com/ms g/message-Firmware-update-87.html	H-CHI-SEMA-180621/414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/415
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/416
semac_d2_n300					
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated.	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31251		
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/418
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/419
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/420
Improper	01-Jun-21	3.5	An XSS vulnerability exists in	https://ww	H-CHI-SEMA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	w.chiyu-tech.com/msg/message-Firmware-update-87.html	180621/421
semac_d4					
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/422
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/423
Improper Neutralization of Input During Web	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-	https://www.chiyu-tech.com/msg/message-	H-CHI-SEMA-180621/424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	Firmware-update-87.html	
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/425
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/426
semac_s1_osdp					
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**		
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/428
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/429
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/431
semac_s2					
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/432
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/434
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/435
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
semac_s3v3					
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/437
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/438
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/439
Integer	01-Jun-21	6.8	A denial of service condition	https://ww	H-CHI-SEMA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	w.chiyu-tech.com/msg/message-Firmware-update-87.html	180621/440
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-SEMA-180621/441
webpass					
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-WEBP-180621/442
Improper Neutralization of Input During Web	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-	https://www.chiyu-tech.com/msg/message-	H-CHI-WEBP-180621/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	Firmware-update-87.html	
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-WEBP-180621/444
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	H-CHI-WEBP-180621/445
Cisco					
asr_5000					
Incorrect Authorization	04-Jun-21	6.5	Multiple vulnerabilities in the authorization process of Cisco ASR 5000 Series Software (StarOS) could allow an authenticated, remote attacker to bypass	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-ASR_-180621/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1539**	sa-asr5k-autho-bypass-mJDF5S7n	
Incorrect Authorization	04-Jun-21	6	Multiple vulnerabilities in the authorization process of Cisco ASR 5000 Series Software (StarOS) could allow an authenticated, remote attacker to bypass authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1540**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-autho-bypass-mJDF5S7n	H-CIS-ASR_-180621/447
asr_5500					
Incorrect Authorization	04-Jun-21	6.5	Multiple vulnerabilities in the authorization process of Cisco ASR 5000 Series Software (StarOS) could allow an authenticated, remote attacker to bypass authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1539**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-autho-bypass-mJDF5S7n	H-CIS-ASR_-180621/448
Incorrect Authorization	04-Jun-21	6	Multiple vulnerabilities in the authorization process of Cisco ASR 5000 Series Software (StarOS) could allow an authenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAd	H-CIS-ASR_-180621/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to bypass authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1540**	visory/cisco-sa-asr5k-autho-bypass-mJDF5S7n	
asr_5700					
Incorrect Authorization	04-Jun-21	6.5	Multiple vulnerabilities in the authorization process of Cisco ASR 5000 Series Software (StarOS) could allow an authenticated, remote attacker to bypass authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1539**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-autho-bypass-mJDF5S7n	H-CIS-ASR_-180621/450
Incorrect Authorization	04-Jun-21	6	Multiple vulnerabilities in the authorization process of Cisco ASR 5000 Series Software (StarOS) could allow an authenticated, remote attacker to bypass authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1540**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-autho-bypass-mJDF5S7n	H-CIS-ASR_-180621/451
vedge_100					
Execution with Unnecessary	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated,	https://tools.cisco.com/security/center	H-CIS-VEDG-180621/452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privileges			local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	
vedge_1000					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	H-CIS-VEDG-180621/453
vedge_100b					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated	https://tools.cisco.com/security/center/content/Cis	H-CIS-VEDG-180621/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	coSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	
vedge_100m					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	H-CIS-VEDG-180621/455
vedge_100wm					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAd	H-CIS-VEDG-180621/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	visory/cisco-sa-sd-wan-fuErCWwF	
vedge_2000					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	H-CIS-VEDG-180621/457
vedge_5000					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-VEDG-180621/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	sa-sd-wan-fuErCWwF	
vedge_cloud					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	H-CIS-VEDG-180621/459
video_surveillance_7070					
Uncontrolled Resource Consumption	04-Jun-21	6.1	Multiple vulnerabilities in the implementation of the Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) for Cisco Video Surveillance 7000 Series IP Cameras could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-	H-CIS-VIDE-180621/460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain Cisco Discovery Protocol and LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted Cisco Discovery Protocol or LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: Cisco Discovery Protocol and LLDP are Layer 2 protocols. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1563**	lldpcdp-mem-yTQDmjRO	
video_surveillance_7530pd					
Uncontrolled Resource Consumption	04-Jun-21	6.1	Multiple vulnerabilities in the implementation of the Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldpcdp-	H-CIS-VIDE-180621/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain Cisco Discovery Protocol and LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted Cisco Discovery Protocol or LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: Cisco Discovery Protocol and LLDP are Layer 2 protocols. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1563**	mem-yTQDmjRO	
Fortinet					
fortiai_3500f					
Improper Input Validation	03-Jun-21	9	An improper input validation in FortiAI v1.4.0 and earlier may allow an authenticated user to gain system shell access via a malicious payload in the "diagnose" command.	https://fortiguard.com/advisory/FG-IR-21-033	H-FOR-FORT-180621/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24023		
Operating System					
Canonical					
ubuntu_linux					
Out-of-bounds Write	04-Jun-21	7.2	The eBPF RINGBUF bpf_ringbuf_reserve() function in the Linux kernel did not check that the allocated size was smaller than the ringbuf size, allowing an attacker to perform out-of-bounds writes within the kernel and therefore, arbitrary code execution. This issue was fixed via commit 4b81ccebaeee ("bpf, ringbuf: Deny reserve of buffers larger than ringbuf") (v5.13-rc4) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. It was introduced via 457f44363a88 ("bpf: Implement BPF ring buffer and verifier support for it") (v5.8-rc1). **CVE ID : CVE-2021-3489**	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf.git/commit/?id=4b81ccebaeee885ab1aa1438133f2991e3a2b6ea	O-CAN-UBUN-180621/463
Out-of-bounds Read	04-Jun-21	7.2	The eBPF ALU32 bounds tracking for bitwise ops (AND, OR and XOR) in the Linux kernel did not properly update 32-bit bounds, which could be turned into out of bounds reads and writes in the Linux kernel and therefore, arbitrary code execution. This issue was fixed via commit 049c4e13714e ("bpf: Fix	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf.git/commit/?id=049c4e13714ecbca567b4d5f6d563f05d431c80e, https://www.openwall.c	O-CAN-UBUN-180621/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			alu32 const subreg bound tracking on bitwise operations") (v5.13-rc4) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. The AND/OR issues were introduced by commit 3f50f132d840 ("bpf: Verifier, do explicit ALU32 bounds tracking") (5.7-rc1) and the XOR variant was introduced by 2921c90d4718 ("bpf:Fix a verifier failure with xor") (5.10-rc1). **CVE ID : CVE-2021-3490**	om/lists/oss-security/2021/05/11/11	
Out-of-bounds Write	04-Jun-21	7.2	The io_uring subsystem in the Linux kernel allowed the MAX_RW_COUNT limit to be bypassed in the PROVIDE_BUFFERS operation, which led to negative values being usedin mem_rw when reading /proc/<PID>/mem. This could be used to create a heap overflow leading to arbitrary code execution in the kernel. It was addressed via commit d1f82808877b ("io_uring: truncate lengths larger than MAX_RW_COUNT on provide buffers") (v5.13-rc1) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. It was introduced in ddf0322db79c ("io_uring: add IORING_OP_PROVIDE_BUFFERS") (v5.7-rc1). **CVE ID : CVE-2021-3491**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=d1f82808877bb10d3deee7cf3374a4eb3fb582db, https://www.openwall.com/lists/oss-security/2021/05/11/13	O-CAN-UBUN-180621/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
chiyu-tech					
bf-430_firmware					
N/A	04-Jun-21	6.4	A CRLF injection vulnerability was found on BF-430, BF-431, and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of validation on the parameter redirect= available on multiple CGI components. **CVE ID : CVE-2021-31249**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-4-180621/466
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-21	3.5	Multiple storage XSS vulnerabilities were discovered on BF-430, BF-431 and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of sanitization of the input on the components man.cgi, if.cgi, dhcpc.cgi, ppp.cgi. **CVE ID : CVE-2021-31250**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.htm	O-CHI-BF-4-180621/467
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-4-180621/468
URL Redirection	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630,	https://www.chiyu-	O-CHI-BF-4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to Untrusted Site ('Open Redirect')			BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	tech.com/msg/message-Firmware-update-87.html	180621/469
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-4-180621/470
bf-431_firmware					
N/A	04-Jun-21	6.4	A CRLF injection vulnerability was found on BF-430, BF-431, and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of validation on the parameter redirect= available on multiple CGI components. **CVE ID : CVE-2021-31249**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-4-180621/471
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-21	3.5	Multiple storage XSS vulnerabilities were discovered on BF-430, BF-431 and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of sanitization of the input on the components man.cgi, if.cgi, dhcpc.cgi,	https://www.chiyu-tech.com/msg/message-Firmware-update-87.htm	O-CHI-BF-4-180621/472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ppp.cgi. **CVE ID : CVE-2021-31250**		
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-4-180621/473
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-4-180621/474
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-4-180621/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bf-450m_firmware					
N/A	04-Jun-21	6.4	A CRLF injection vulnerability was found on BF-430, BF-431, and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of validation on the parameter redirect= available on multiple CGI components. **CVE ID : CVE-2021-31249**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-4-180621/476
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-21	3.5	Multiple storage XSS vulnerabilities were discovered on BF-430, BF-431 and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of sanitization of the input on the components man.cgi, if.cgi, dhcpc.cgi, ppp.cgi. **CVE ID : CVE-2021-31250**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.htm	O-CHI-BF-4-180621/477
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-4-180621/478
URL Redirection to Untrusted	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431,	https://www.chiyu-tech.com/ms	O-CHI-BF-4-180621/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	g/message-Firmware-update-87.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-4-180621/480
bf-630_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-6-180621/481
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-6-180621/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**		
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-6-180621/483
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-6-180621/484
bf-631w_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it.	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-6-180621/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31252		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-6-180621/486
bf-631_firmware					
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-6-180621/487
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-6-180621/488
bf-830w_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-8-180621/489
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BF-8-180621/490
bfminiw_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BFMI-180621/491
biosense_firmware					
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU	https://www.chiyu-tech.com/msg/message-	O-CHI-BIOS-180621/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	Firmware-update-87.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-BIOS-180621/493
semac_d1_firmware					
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/494
URL Redirection to Untrusted	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431,	https://www.chiyu-tech.com/ms	O-CHI-SEMA-180621/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	g/message-Firmware-update-87.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/496
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/497
Improper Neutralization of Input During Web Page	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a	https://www.chiyu-tech.com/msg/message-Firmware-	O-CHI-SEMA-180621/498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	update-87.html	
semac_d2_firmware					
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/499
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/500
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**		
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/502
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/503
semac_d2_n300_firmware					
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**		
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/505
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/506
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reboot of the device. **CVE ID : CVE-2021-31642**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/508
semac_d4_firmware					
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/509
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/511
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/512
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/513
semac_s1_osdp_firmware					
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP	https://www.chiyu-tech.com/ms	O-CHI-SEMA-180621/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	g/message-Firmware-update-87.html	
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/515
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/516
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including	https://www.chiyu-tech.com/msg/message-Firmware-	O-CHI-SEMA-180621/517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	update-87.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/518
semac_s2_firmware					
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/519
URL Redirection to Untrusted Site ('Open	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W,	https://www.chiyu-tech.com/msg/message-	O-CHI-SEMA-180621/520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redirect')			Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	Firmware-update-87.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/521
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/522
Improper Neutralization of Input During Web Page Generation	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the	https://www.chiyu-tech.com/msg/message-Firmware-update-	O-CHI-SEMA-180621/523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	87.html	
semac_s3v3_firmware					
Improper Authentication	04-Jun-21	7.5	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated. **CVE ID : CVE-2021-31251**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/524
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/525
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			404 message is generated. **CVE ID : CVE-2021-31641**		
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/527
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-SEMA-180621/528
webpass_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	04-Jun-21	5.8	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it. **CVE ID : CVE-2021-31252**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-WEBP-180621/529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	4.3	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated. **CVE ID : CVE-2021-31641**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-WEBP-180621/530
Integer Overflow or Wraparound	01-Jun-21	6.8	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device. **CVE ID : CVE-2021-31642**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-WEBP-180621/531
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-21	3.5	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter. **CVE ID : CVE-2021-31643**	https://www.chiyu-tech.com/msg/message-Firmware-update-87.html	O-CHI-WEBP-180621/532
Cisco					
staros					
Incorrect Authorizatio	04-Jun-21	6.5	Multiple vulnerabilities in the authorization process of	https://tools.cisco.com/se	O-CIS-STAR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			Cisco ASR 5000 Series Software (StarOS) could allow an authenticated, remote attacker to bypass authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1539**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-autho-bypass-mJDF5S7n	180621/533
Incorrect Authorization	04-Jun-21	6	Multiple vulnerabilities in the authorization process of Cisco ASR 5000 Series Software (StarOS) could allow an authenticated, remote attacker to bypass authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1540**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-autho-bypass-mJDF5S7n	O-CIS-STAR-180621/534
vedge_1000_firmware					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	O-CIS-VEDG-180621/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			actions with the privileges of the root user. **CVE ID : CVE-2021-1528**		
vedge_100b_firmware					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	O-CIS-VEDG-180621/536
vedge_100m_firmware					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	O-CIS-VEDG-180621/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the root user. **CVE ID : CVE-2021-1528**		
vedge_100wm_firmware					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	O-CIS-VEDG-180621/538
vedge_100_firmware					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	O-CIS-VEDG-180621/539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1528		
vedge_2000_firmware					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	O-CIS-VEDG-180621/540
vedge_5000_firmware					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	O-CIS-VEDG-180621/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vedge_cloud_firmware					
Execution with Unnecessary Privileges	04-Jun-21	7.2	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user. **CVE ID : CVE-2021-1528**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF	O-CIS-VEDG-180621/542
video_surveillance_7070_firmware					
Uncontrolled Resource Consumption	04-Jun-21	6.1	Multiple vulnerabilities in the implementation of the Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain Cisco Discovery Protocol and LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted Cisco Discovery	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldpcdp-mem-yTQDmjRO	O-CIS-VIDE-180621/543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol or LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: Cisco Discovery Protocol and LLDP are Layer 2 protocols. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1563**		
video_surveillance_7530pd_firmware					
Uncontrolled Resource Consumption	04-Jun-21	6.1	Multiple vulnerabilities in the implementation of the Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain Cisco Discovery Protocol and LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted Cisco Discovery Protocol or LLDP packets to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldpcdp-mem-yTQDmjRO	O-CIS-VIDE-180621/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: Cisco Discovery Protocol and LLDP are Layer 2 protocols. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1563**		
Debian					
debian_linux					
Use After Free	01-Jun-21	6.8	There's a flaw in libxml2's xmllint in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by xmllint could trigger a use-after-free. The greatest impact of this flaw is to confidentiality, integrity, and availability. **CVE ID : CVE-2021-3516**	https://gitlab.gnome.org/GNOME/libxml2/-/commit/1358d157d0bd83be1dfe356a69213df9fac0b539	O-DEB-DEBI-180621/545
Improper Verification of Cryptographic Signature	04-Jun-21	5	Lasso all versions prior to 2.7.0 has improper verification of a cryptographic signature. **CVE ID : CVE-2021-28091**	https://git.entrouvert.org/lasso.git/commit/?id=076a37d7f0eb74001127481da2d355683693cde9, https://git.entrouvert.or	O-DEB-DEBI-180621/546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				g/lasso.git/tree/NEWS?id=v2.7.0	
Fedoraproject					
fedora					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jun-21	6.5	Redis is an open source (BSD licensed), in-memory data structure store, used as a database, cache, and message broker. An integer overflow bug in Redis version 6.0 or newer (on 32-bit systems ONLY) can be exploited using the `STRALGO LCS` command to corrupt the heap and potentially result with remote code execution. This is a result of an incomplete fix for CVE-2021-29477 which only addresses the problem on 64-bit systems but fails to do that for 32-bit. 64-bit systems are not affected. The problem is fixed in version 6.2.4 and 6.0.14. An additional workaround to mitigate the problem without patching the `redis-server` executable is to use ACL configuration to prevent clients from using the `STRALGO LCS` command. **CVE ID : CVE-2021-32625**	https://github.com/redis/redis/security/advisories/GHSA-46cp-x4x9-6pfq	O-FED-FEDO-180621/547
Use After Free	01-Jun-21	6.8	There's a flaw in libxml2's xmllint in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by xmllint could trigger a use-after-free. The greatest impact of this flaw is	https://gitlab.gnome.org/GNOME/libxml2/-/commit/1358d157d0bd83be1dfe356	O-FED-FEDO-180621/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to confidentiality, integrity, and availability. **CVE ID : CVE-2021-3516**	a69213df9fac0b539	
NULL Pointer Dereference	01-Jun-21	7.2	A flaw null pointer dereference in the Nitro Enclaves kernel driver was found in the way that Enclaves VMs forces closures on the enclave file descriptor. A local user of a host machine could use this flaw to crash the system or escalate their privileges on the system. **CVE ID : CVE-2021-3543**	N/A	O-FED-FEDO-180621/549
Out-of-bounds Write	08-Jun-21	6.8	A heap-buffer overflow was found in the copyIntoFrameBuffer function of OpenEXR in versions before 3.0.1. An attacker could use this flaw to execute arbitrary code with the permissions of the user running the application compiled against OpenEXR. **CVE ID : CVE-2021-23169**	N/A	O-FED-FEDO-180621/550
Integer Overflow or Wraparound	08-Jun-21	4.3	An integer overflow leading to a heap-buffer overflow was found in the DwaCompressor of OpenEXR in versions before 3.0.1. An attacker could use this flaw to crash an application compiled with OpenEXR. **CVE ID : CVE-2021-23215**	N/A	O-FED-FEDO-180621/551
Out-of-bounds Read	02-Jun-21	6.4	An issue was discovered in Pillow before 8.2.0. There is an out-of-bounds read in J2kDecode, in j2ku_graya_la.	https://pillow.readthedocs.io/en/stable/releasenotes/8.2.0.html	O-FED-FEDO-180621/552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25287	#cve-2021-25287-cve-2021-25288-fix-oob-read-in-jpeg2kdecode	
Out-of-bounds Read	02-Jun-21	6.4	An issue was discovered in Pillow before 8.2.0. There is an out-of-bounds read in J2kDecode, in j2ku_gray_i. **CVE ID : CVE-2021-25288**	https://pillow.readthedocs.io/en/stable/releasenotes/8.2.0.html#cve-2021-25287-cve-2021-25288-fix-oob-read-in-jpeg2kdecode	O-FED-FEDO-180621/553
Integer Underflow (Wrap or Wraparound)	08-Jun-21	4.3	An integer overflow leading to a heap-buffer overflow was found in the DwaCompressor of OpenEXR in versions before 3.0.1. An attacker could use this flaw to crash an application compiled with OpenEXR. This is a different flaw from CVE-2021-23215. **CVE ID : CVE-2021-26260**	N/A	O-FED-FEDO-180621/554
Unchecked Return Value	02-Jun-21	4.3	An issue was discovered in Pillow before 8.2.0. PSDImagePlugin.PsdImageFile lacked a sanity check on the number of input layers relative to the size of the data block. This could lead to a DoS on Image.open prior to Image.load. **CVE ID : CVE-2021-28675**	https://pillow.readthedocs.io/en/stable/releasenotes/8.2.0.html#cve-2021-28675-fix-dos-in-psdimageplugin	O-FED-FEDO-180621/555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jun-21	5	An issue was discovered in Pillow before 8.2.0. For FLI data, FliDecode did not properly check that the block advance was non-zero, potentially leading to an infinite loop on load. **CVE ID : CVE-2021-28676**	N/A	O-FED-FEDO-180621/556
N/A	02-Jun-21	5	An issue was discovered in Pillow before 8.2.0. For EPS data, the readline implementation used in EPSImageFile has to deal with any combination of \r and \n as line endings. It used an accidentally quadratic method of accumulating lines while looking for a line ending. A malicious EPS file could use this to perform a DoS of Pillow in the open phase, before an image was accepted for opening. **CVE ID : CVE-2021-28677**	https://github.com/python-pillow/Pillow/pull/5377	O-FED-FEDO-180621/557
Insufficient Verification of Data Authenticity	02-Jun-21	4.3	An issue was discovered in Pillow before 8.2.0. For BLP data, BlpImagePlugin did not properly check that reads (after jumping to file offsets) returned data. This could lead to a DoS where the decoder could be run a large number of times on empty data. **CVE ID : CVE-2021-28678**	https://github.com/python-pillow/Pillow/pull/5377, https://pillow.readthedocs.io/en/stable/releasenotes/8.2.0.html#cve-2021-28678-fix-blp-dos	O-FED-FEDO-180621/558
Fortinet					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fortiai_firmware					
Improper Input Validation	03-Jun-21	9	An improper input validation in FortiAI v1.4.0 and earlier may allow an authenticated user to gain system shell access via a malicious payload in the "diagnose" command. **CVE ID : CVE-2021-24023**	https://fortiguard.com/advisory/FG-IR-21-033	O-FOR-FORT-180621/559
fortios					
Improper Certificate Validation	02-Jun-21	7.5	An improper following of a certificate's chain of trust vulnerability in FortiGate versions 6.4.0 to 6.4.4 may allow an LDAP user to connect to SSLVPN with any certificate that is signed by a trusted Certificate Authority. **CVE ID : CVE-2021-24012**	https://fortiguard.com/advisory/FG-IR-21-018	O-FOR-FORT-180621/560
fortiswitch					
Missing Release of Memory after Effective Lifetime	01-Jun-21	3.3	A missing release of memory after effective lifetime vulnerability in FortiSwitch 6.4.0 to 6.4.6, 6.2.0 to 6.2.6, 6.0.0 to 6.0.6, 3.6.11 and below may allow an attacker on an adjacent network to exhaust available memory by sending specifically crafted LLDP/CDP/EDP packets to the device. **CVE ID : CVE-2021-26111**	https://fortiguard.com/advisory/FG-IR-21-026	O-FOR-FORT-180621/561
Google					
android					
Improper Neutralization of Special Elements in	04-Jun-21	6.8	Incorrect security UI in Web App Installs in Google Chrome on Android prior to 90.0.4430.212 allowed an	https://crbug.com/1180126, https://chro	O-GOO-ANDR-180621/562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Output Used by a Downstream Component ('Injection')			attacker who convinced a user to install a web application to inject scripts or HTML into a privileged page via a crafted HTML page. **CVE ID : CVE-2021-30506**	mereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html	
Inclusion of Functionality from Untrusted Control Sphere	04-Jun-21	6.8	Inappropriate implementation in Offline in Google Chrome on Android prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. **CVE ID : CVE-2021-30507**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html, https://crbug.com/1178202	O-GOO-ANDR-180621/563
Out-of-bounds Write	07-Jun-21	6.8	Heap buffer overflow in Autofill in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. **CVE ID : CVE-2021-30521**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	O-GOO-ANDR-180621/564
Use After Free	07-Jun-21	6.8	Use after free in WebAuthentication in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker who had compromised the renderer process of a user who had saved a credit card in their Google account to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30528**	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html	O-GOO-ANDR-180621/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	11-Jun-21	5	In startIpClient of ClientModeImpl.java, there is a possible identifier which could be used to track a device. This could lead to remote information disclosure to a proximal attacker, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-154114734 **CVE ID : CVE-2021-0466**	https://source.android.com/security/bulletin/2021-05-01	O-GOO-ANDR-180621/566
Improper Privilege Management	11-Jun-21	4.6	In shouldLockKeyguard of LockTaskController.java, there is a possible way to exit App Pinning without a PIN due to a permissions bypass. 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-9 Android-10Android ID: A-176801033 **CVE ID : CVE-2021-0472**	https://source.android.com/security/bulletin/2021-05-01	O-GOO-ANDR-180621/567
Double Free	11-Jun-21	8.3	In rw_t3t_process_error of rw_t3t.cc, there is a possible double free due to uninitialized data. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2021-05-01	O-GOO-ANDR-180621/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-179687208 **CVE ID : CVE-2021-0473**		
Out-of-bounds Write	11-Jun-21	10	In avrc_msg_cback of avrc_api.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution 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-177611958 **CVE ID : CVE-2021-0474**	https://source.android.com/security/bulletin/2021-05-01	O-GOO-ANDR-180621/569
Use After Free	11-Jun-21	8.3	In on_l2cap_data_ind of btif_sock_l2cap.cc, there is possible memory corruption due to a use after free. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-175686168 **CVE ID : CVE-2021-0475**	https://source.android.com/security/bulletin/2021-05-01	O-GOO-ANDR-180621/570
Linux					
linux_kernel					
Out-of-bounds	04-Jun-21	7.2	The eBPF RINGBUF bpf_ringbuf_reserve() function in the Linux kernel	https://git.kernel.org/pub/scm/linux	O-LIN-LINU-180621/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			did not check that the allocated size was smaller than the ringbuf size, allowing an attacker to perform out-of-bounds writes within the kernel and therefore, arbitrary code execution. This issue was fixed via commit 4b81ccebaeee ("bpf, ringbuf: Deny reserve of buffers larger than ringbuf") (v5.13-rc4) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. It was introduced via 457f44363a88 ("bpf: Implement BPF ring buffer and verifier support for it") (v5.8-rc1). **CVE ID : CVE-2021-3489**	/kernel/git/bpf/bpf.git/commit/?id=4b81ccebaeee885ab1aa1438133f2991e3a2b6ea	
Out-of-bounds Read	04-Jun-21	7.2	The eBPF ALU32 bounds tracking for bitwise ops (AND, OR and XOR) in the Linux kernel did not properly update 32-bit bounds, which could be turned into out of bounds reads and writes in the Linux kernel and therefore, arbitrary code execution. This issue was fixed via commit 049c4e13714e ("bpf: Fix alu32 const subreg bound tracking on bitwise operations") (v5.13-rc4) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. The AND/OR issues were introduced by commit 3f50f132d840 ("bpf: Verifier, do explicit ALU32	https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf.git/commit/?id=049c4e13714ecbca567b4d5f6d563f05d431c80e, https://www.openwall.com/lists/oss-security/2021/05/11/11	O-LIN-LINU-180621/572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bounds tracking") (5.7-rc1) and the XOR variant was introduced by 2921c90d4718 ("bpf:Fix a verifier failure with xor") (5.10-rc1). **CVE ID : CVE-2021-3490**		
Out-of-bounds Write	04-Jun-21	7.2	The io_uring subsystem in the Linux kernel allowed the MAX_RW_COUNT limit to be bypassed in the PROVIDE_BUFFERS operation, which led to negative values being usedin mem_rw when reading /proc/<PID>/mem. This could be used to create a heap overflow leading to arbitrary code execution in the kernel. It was addressed via commit d1f82808877b ("io_uring: truncate lengths larger than MAX_RW_COUNT on provide buffers") (v5.13-rc1) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. It was introduced in ddf0322db79c ("io_uring: add IORING_OP_PROVIDE_BUFFERS") (v5.7-rc1). **CVE ID : CVE-2021-3491**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=d1f82808877bb10d3deee7cf3374a4eb3fb582db, https://www.openwall.com/lists/oss-security/2021/05/11/13	O-LIN-LINU-180621/573
Microsoft					
windows_10					
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	2.1	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2021-31955**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-180621/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-31955	
Improper Privilege Management	08-Jun-21	9.3	Windows NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31956**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31956	O-MIC-WIND-180621/575
Improper Privilege Management	08-Jun-21	6.8	Windows NTLM Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31958**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31958	O-MIC-WIND-180621/576
N/A	08-Jun-21	6.8	Scripting Engine Memory Corruption Vulnerability **CVE ID : CVE-2021-31959**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31959	O-MIC-WIND-180621/577
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	2.1	Windows Bind Filter Driver Information Disclosure Vulnerability **CVE ID : CVE-2021-31960**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31960	O-MIC-WIND-180621/578
N/A	08-Jun-21	7.5	Kerberos AppContainer Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31962**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31962	O-MIC-WIND-180621/579
N/A	08-Jun-21	5	Windows Remote Desktop ServicesÂ Denial of Service Vulnerability	https://portal.msrc.microsoft.com/en	O-MIC-WIND-180621/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31968	-US/security-guidance/advisory/CVE-2021-31968	
Improper Privilege Management	08-Jun-21	4.6	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31969**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31969	O-MIC-WIND-180621/581
N/A	08-Jun-21	2.1	Windows TCP/IP Driver Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31970	O-MIC-WIND-180621/582
N/A	08-Jun-21	6.8	Windows HTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31971**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31971	O-MIC-WIND-180621/583
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	2.1	Event Tracing for Windows Information Disclosure Vulnerability **CVE ID : CVE-2021-31972**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31972	O-MIC-WIND-180621/584
Improper Privilege Management	08-Jun-21	4.6	Windows GPSVC Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31973	O-MIC-WIND-180621/585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Jun-21	5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2021-31974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31974	O-MIC-WIND-180621/586
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	7.8	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31976. **CVE ID : CVE-2021-31975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31975	O-MIC-WIND-180621/587
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	7.8	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31975. **CVE ID : CVE-2021-31976**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31976	O-MIC-WIND-180621/588
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Jun-21	5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2021-31977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31977	O-MIC-WIND-180621/589
Improper Privilege Management	08-Jun-21	4.6	Microsoft DWM Core Library Elevation of Privilege Vulnerability **CVE ID : CVE-2021-33739**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33739	O-MIC-WIND-180621/590
N/A	08-Jun-21	6.8	Windows MSHTML Platform Remote Code Execution Vulnerability	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180621/591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-33742	guidance/advisory/CVE-2021-33742	
windows_7					
Improper Privilege Management	08-Jun-21	9.3	Windows NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31956**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31956	O-MIC-WIND-180621/592
Improper Privilege Management	08-Jun-21	6.8	Windows NTLM Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31958**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31958	O-MIC-WIND-180621/593
N/A	08-Jun-21	6.8	Scripting Engine Memory Corruption Vulnerability **CVE ID : CVE-2021-31959**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31959	O-MIC-WIND-180621/594
N/A	08-Jun-21	7.5	Kerberos AppContainer Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31962**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31962	O-MIC-WIND-180621/595
N/A	08-Jun-21	5	Windows Remote Desktop ServicesÂ Denial of Service Vulnerability **CVE ID : CVE-2021-31968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31968	O-MIC-WIND-180621/596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Jun-21	6.8	Windows HTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31971**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31971	O-MIC-WIND-180621/597
Improper Privilege Management	08-Jun-21	4.6	Windows GPSVC Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31973	O-MIC-WIND-180621/598
N/A	08-Jun-21	6.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2021-33742**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33742	O-MIC-WIND-180621/599
windows_8.1					
Improper Privilege Management	08-Jun-21	9.3	Windows NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31956**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31956	O-MIC-WIND-180621/600
Improper Privilege Management	08-Jun-21	6.8	Windows NTLM Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31958**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31958	O-MIC-WIND-180621/601
N/A	08-Jun-21	6.8	Scripting Engine Memory Corruption Vulnerability **CVE ID : CVE-2021-31959**	https://portal.msrc.microsoft.com/en	O-MIC-WIND-180621/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				-US/security-guidance/advisory/CVE-2021-31959	
N/A	08-Jun-21	7.5	Kerberos AppContainer Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31962**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31962	O-MIC-WIND-180621/603
N/A	08-Jun-21	5	Windows Remote Desktop ServicesÂ Denial of Service Vulnerability **CVE ID : CVE-2021-31968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31968	O-MIC-WIND-180621/604
N/A	08-Jun-21	2.1	Windows TCP/IP Driver Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31970	O-MIC-WIND-180621/605
N/A	08-Jun-21	6.8	Windows HTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31971**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31971	O-MIC-WIND-180621/606
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	2.1	Event Tracing for Windows Information Disclosure Vulnerability **CVE ID : CVE-2021-31972**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31972	O-MIC-WIND-180621/607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	08-Jun-21	4.6	Windows GPSVC Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31973	O-MIC-WIND-180621/608
N/A	08-Jun-21	5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2021-31974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31974	O-MIC-WIND-180621/609
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	7.8	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31976. **CVE ID : CVE-2021-31975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31975	O-MIC-WIND-180621/610
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	7.8	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31975. **CVE ID : CVE-2021-31976**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31976	O-MIC-WIND-180621/611
N/A	08-Jun-21	6.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2021-33742**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33742	O-MIC-WIND-180621/612
windows_rt_8.1					
Improper Privilege Management	08-Jun-21	9.3	Windows NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31956**	https://portal.msrc.microsoft.com/en	O-MIC-WIND-180621/613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				-US/security-guidance/advisory/CVE-2021-31956	
Improper Privilege Management	08-Jun-21	6.8	Windows NTLM Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31958**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31958	O-MIC-WIND-180621/614
N/A	08-Jun-21	6.8	Scripting Engine Memory Corruption Vulnerability **CVE ID : CVE-2021-31959**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31959	O-MIC-WIND-180621/615
N/A	08-Jun-21	7.5	Kerberos AppContainer Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31962**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31962	O-MIC-WIND-180621/616
N/A	08-Jun-21	5	Windows Remote Desktop ServicesÂ Denial of Service Vulnerability **CVE ID : CVE-2021-31968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31968	O-MIC-WIND-180621/617
N/A	08-Jun-21	2.1	Windows TCP/IP Driver Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31970	O-MIC-WIND-180621/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Jun-21	6.8	Windows HTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31971**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31971	O-MIC-WIND-180621/619
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	2.1	Event Tracing for Windows Information Disclosure Vulnerability **CVE ID : CVE-2021-31972**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31972	O-MIC-WIND-180621/620
Improper Privilege Management	08-Jun-21	4.6	Windows GPSVC Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31973	O-MIC-WIND-180621/621
N/A	08-Jun-21	5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2021-31974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31974	O-MIC-WIND-180621/622
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	7.8	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31976. **CVE ID : CVE-2021-31975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31975	O-MIC-WIND-180621/623
Exposure of Sensitive Information to an Unauthorize	08-Jun-21	7.8	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31975.	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-180621/624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Actor			**CVE ID : CVE-2021-31976**	visory/CVE-2021-31976	
N/A	08-Jun-21	6.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2021-33742**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33742	O-MIC-WIND-180621/625
windows_server_2008					
Improper Privilege Management	08-Jun-21	4.6	Microsoft Enhanced Cryptographic Provider Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31199. **CVE ID : CVE-2021-31201**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31201	O-MIC-WIND-180621/626
Improper Privilege Management	08-Jun-21	9.3	Windows NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31956**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31956	O-MIC-WIND-180621/627
Improper Privilege Management	08-Jun-21	6.8	Windows NTLM Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31958**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31958	O-MIC-WIND-180621/628
N/A	08-Jun-21	6.8	Scripting Engine Memory Corruption Vulnerability **CVE ID : CVE-2021-31959**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31959	O-MIC-WIND-180621/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Jun-21	7.5	Kerberos AppContainer Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31962**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31962	O-MIC-WIND-180621/630
N/A	08-Jun-21	5	Windows Remote Desktop ServicesÂ Denial of Service Vulnerability **CVE ID : CVE-2021-31968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31968	O-MIC-WIND-180621/631
N/A	08-Jun-21	6.8	Windows HTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31971**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31971	O-MIC-WIND-180621/632
Improper Privilege Management	08-Jun-21	4.6	Windows GPSVC Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31973	O-MIC-WIND-180621/633
N/A	08-Jun-21	6.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2021-33742**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33742	O-MIC-WIND-180621/634
Improper Privilege Management	08-Jun-21	6.8	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID : CVE-2021-1675**	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-180621/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visory/CVE-2021-1675	
N/A	08-Jun-21	4.3	Windows DCOM Server Security Feature Bypass **CVE ID : CVE-2021-26414**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26414	O-MIC-WIND-180621/636
windows_server_2012					
Improper Privilege Management	08-Jun-21	4.6	Microsoft Enhanced Cryptographic Provider Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31199. **CVE ID : CVE-2021-31201**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31201	O-MIC-WIND-180621/637
Improper Privilege Management	08-Jun-21	9.3	Windows NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31956**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31956	O-MIC-WIND-180621/638
Improper Privilege Management	08-Jun-21	6.8	Windows NTLM Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31958**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31958	O-MIC-WIND-180621/639
N/A	08-Jun-21	6.8	Scripting Engine Memory Corruption Vulnerability **CVE ID : CVE-2021-31959**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31959	O-MIC-WIND-180621/640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Jun-21	7.5	Kerberos AppContainer Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31962**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31962	O-MIC-WIND-180621/641
N/A	08-Jun-21	5	Windows Remote Desktop ServicesÂ Denial of Service Vulnerability **CVE ID : CVE-2021-31968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31968	O-MIC-WIND-180621/642
N/A	08-Jun-21	2.1	Windows TCP/IP Driver Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31970	O-MIC-WIND-180621/643
N/A	08-Jun-21	6.8	Windows HTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31971**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31971	O-MIC-WIND-180621/644
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	2.1	Event Tracing for Windows Information Disclosure Vulnerability **CVE ID : CVE-2021-31972**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31972	O-MIC-WIND-180621/645
Improper Privilege Management	08-Jun-21	4.6	Windows GPSVC Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31973**	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-180621/646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visory/CVE-2021-31973	
N/A	08-Jun-21	5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2021-31974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31974	O-MIC-WIND-180621/647
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	7.8	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31976. **CVE ID : CVE-2021-31975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31975	O-MIC-WIND-180621/648
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	7.8	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31975. **CVE ID : CVE-2021-31976**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31976	O-MIC-WIND-180621/649
N/A	08-Jun-21	6.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2021-33742**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33742	O-MIC-WIND-180621/650
Improper Privilege Management	08-Jun-21	6.8	Windows Print Spooler Elevation of Privilege Vulnerability **CVE ID : CVE-2021-1675**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1675	O-MIC-WIND-180621/651
N/A	08-Jun-21	4.3	Windows DCOM Server Security Feature Bypass	https://portal.msrc.micr	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26414	osoft.com/en-US/security-guidance/advisory/CVE-2021-26414	180621/652
windows_server_2016					
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	2.1	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2021-31955**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31955	O-MIC-WIND-180621/653
Improper Privilege Management	08-Jun-21	9.3	Windows NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31956**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31956	O-MIC-WIND-180621/654
Improper Privilege Management	08-Jun-21	6.8	Windows NTLM Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31958**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31958	O-MIC-WIND-180621/655
N/A	08-Jun-21	6.8	Scripting Engine Memory Corruption Vulnerability **CVE ID : CVE-2021-31959**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31959	O-MIC-WIND-180621/656
Exposure of Sensitive Information to an Unauthorize	08-Jun-21	2.1	Windows Bind Filter Driver Information Disclosure Vulnerability **CVE ID : CVE-2021-31960**	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-180621/657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Actor				visory/CVE-2021-31960	
N/A	08-Jun-21	7.5	Kerberos AppContainer Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31962**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31962	O-MIC-WIND-180621/658
N/A	08-Jun-21	5	Windows Remote Desktop ServicesÂ Denial of Service Vulnerability **CVE ID : CVE-2021-31968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31968	O-MIC-WIND-180621/659
Improper Privilege Management	08-Jun-21	4.6	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31969**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31969	O-MIC-WIND-180621/660
N/A	08-Jun-21	2.1	Windows TCP/IP Driver Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31970	O-MIC-WIND-180621/661
N/A	08-Jun-21	6.8	Windows HTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31971**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31971	O-MIC-WIND-180621/662
Exposure of Sensitive	08-Jun-21	2.1	Event Tracing for Windows Information Disclosure	https://portal.msrc.micr	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information to an Unauthorized Actor			Vulnerability **CVE ID : CVE-2021-31972**	osoft.com/en-US/security-guidance/advisory/CVE-2021-31972	180621/663
Improper Privilege Management	08-Jun-21	4.6	Windows GPSVC Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31973	O-MIC-WIND-180621/664
N/A	08-Jun-21	5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2021-31974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31974	O-MIC-WIND-180621/665
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	7.8	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31976. **CVE ID : CVE-2021-31975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31975	O-MIC-WIND-180621/666
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	7.8	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31975. **CVE ID : CVE-2021-31976**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31976	O-MIC-WIND-180621/667
Improper Restriction of Operations within the Bounds of a Memory	08-Jun-21	5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2021-31977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-180621/668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer				2021-31977	
Improper Privilege Management	08-Jun-21	4.6	Microsoft DWM Core Library Elevation of Privilege Vulnerability **CVE ID : CVE-2021-33739**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33739	O-MIC-WIND-180621/669
N/A	08-Jun-21	6.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2021-33742**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33742	O-MIC-WIND-180621/670
windows_server_2019					
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	2.1	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2021-31955**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31955	O-MIC-WIND-180621/671
Improper Privilege Management	08-Jun-21	9.3	Windows NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31956**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31956	O-MIC-WIND-180621/672
Improper Privilege Management	08-Jun-21	6.8	Windows NTLM Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31958**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31958	O-MIC-WIND-180621/673
N/A	08-Jun-21	6.8	Scripting Engine Memory Corruption Vulnerability	https://portal.msrc.micr	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31959	osoft.com/en-US/security-guidance/advisory/CVE-2021-31959	180621/674
N/A	08-Jun-21	7.5	Kerberos AppContainer Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31962**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31962	O-MIC-WIND-180621/675
N/A	08-Jun-21	5	Windows Remote Desktop ServicesÂ Denial of Service Vulnerability **CVE ID : CVE-2021-31968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31968	O-MIC-WIND-180621/676
Improper Privilege Management	08-Jun-21	4.6	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31969**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31969	O-MIC-WIND-180621/677
N/A	08-Jun-21	2.1	Windows TCP/IP Driver Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31970	O-MIC-WIND-180621/678
N/A	08-Jun-21	6.8	Windows HTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2021-31971**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-180621/679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-31971	
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	2.1	Event Tracing for Windows Information Disclosure Vulnerability **CVE ID : CVE-2021-31972**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31972	O-MIC-WIND-180621/680
Improper Privilege Management	08-Jun-21	4.6	Windows GPSVC Elevation of Privilege Vulnerability **CVE ID : CVE-2021-31973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31973	O-MIC-WIND-180621/681
N/A	08-Jun-21	5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2021-31974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31974	O-MIC-WIND-180621/682
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	7.8	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31976. **CVE ID : CVE-2021-31975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31975	O-MIC-WIND-180621/683
Exposure of Sensitive Information to an Unauthorized Actor	08-Jun-21	7.8	Server for NFS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-31975. **CVE ID : CVE-2021-31976**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31976	O-MIC-WIND-180621/684
Improper Restriction of	08-Jun-21	5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2021-31977**	https://portal.msrc.microsoft.com/en	O-MIC-WIND-180621/685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer				-US/security-guidance/advisory/CVE-2021-31977	
N/A	08-Jun-21	6.8	Windows MSHTML Platform Remote Code Execution Vulnerability **CVE ID : CVE-2021-33742**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33742	O-MIC-WIND-180621/686
Netapp					
clustered_data_ontap					
N/A	04-Jun-21	4	Clustered Data ONTAP versions prior to 9.7P13 and 9.8P3 are susceptible to a vulnerability which could allow single workloads to cause a Denial of Service (DoS) on a cluster node. **CVE ID : CVE-2021-26994**	https://security.netapp.com/advisory/NTAP-20210601-0001/	O-NET-CLUS-180621/687
Qnap					
qts					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-21	3.5	A DOM-based XSS vulnerability has been reported to affect QNAP NAS running QTS and QuTS hero. If exploited, this vulnerability allows attackers to inject malicious code. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.3.1652 Build 20210428. QNAP Systems Inc. QuTS hero versions prior to h4.5.2.1638 Build 20210414. QNAP Systems Inc. QuTScloud versions prior to c4.5.5.1656	https://www.qnap.com/zh-tw/security-advisory/qsa-21-22	O-QNA-QTS-180621/688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Build 20210503. This issue does not affect: QNAP Systems Inc. QTS 4.3.6; 4.3.3. **CVE ID : CVE-2021-28806**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-21	3.5	A post-authentication reflected XSS vulnerability has been reported to affect QNAP NAS running Q'center. If exploited, this vulnerability allows remote attackers to inject malicious code. QNAP have already fixed this vulnerability in the following versions of Q'center: QTS 4.5.3: Q'center v1.12.1012 and later QTS 4.3.6: Q'center v1.10.1004 and later QTS 4.3.3: Q'center v1.10.1004 and later QuTS hero h4.5.2: Q'center v1.12.1012 and later QuTScloud c4.5.4: Q'center v1.12.1012 and later **CVE ID : CVE-2021-28807**	https://www.qnap.com/zh-tw/security-advisory/qsa-21-20	O-QNA-QTS-180621/689
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Jun-21	6.5	A command injection vulnerability has been reported to affect certain versions of Video Station. If exploited, this vulnerability allows remote attackers to execute arbitrary commands. This issue affects: QNAP Systems Inc. Video Station versions prior to 5.5.4 on QTS 4.5.2; versions prior to 5.5.4 on QuTS hero h4.5.2; versions prior to 5.5.4 on QuTScloud c4.5.4. This issue does not affect: QNAP Systems Inc. Video Station on QTS 4.3.6; on QTS 4.3.3.	https://www.qnap.com/zh-tw/security-advisory/qsa-21-21	O-QNA-QTS-180621/690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28812		
qutscloud					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-21	3.5	A DOM-based XSS vulnerability has been reported to affect QNAP NAS running QTS and QuTS hero. If exploited, this vulnerability allows attackers to inject malicious code. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.3.1652 Build 20210428. QNAP Systems Inc. QuTS hero versions prior to h4.5.2.1638 Build 20210414. QNAP Systems Inc. QuTScloud versions prior to c4.5.5.1656 Build 20210503. This issue does not affect: QNAP Systems Inc. QTS 4.3.6; 4.3.3. **CVE ID : CVE-2021-28806**	https://www.qnap.com/zh-tw/security-advisory/qsa-21-22	O-QNA-QUTS-180621/691
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-21	3.5	A post-authentication reflected XSS vulnerability has been reported to affect QNAP NAS running Q'center. If exploited, this vulnerability allows remote attackers to inject malicious code. QNAP have already fixed this vulnerability in the following versions of Q'center: QTS 4.5.3: Q'center v1.12.1012 and later QTS 4.3.6: Q'center v1.10.1004 and later QTS 4.3.3: Q'center v1.10.1004 and later QuTS hero h4.5.2: Q'center v1.12.1012 and later QuTScloud c4.5.4: Q'center v1.12.1012 and later	https://www.qnap.com/zh-tw/security-advisory/qsa-21-20	O-QNA-QUTS-180621/692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28807		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Jun-21	6.5	A command injection vulnerability has been reported to affect certain versions of Video Station. If exploited, this vulnerability allows remote attackers to execute arbitrary commands. This issue affects: QNAP Systems Inc. Video Station versions prior to 5.5.4 on QTS 4.5.2; versions prior to 5.5.4 on QuTS hero h4.5.2; versions prior to 5.5.4 on QuTScloud c4.5.4. This issue does not affect: QNAP Systems Inc. Video Station on QTS 4.3.6; on QTS 4.3.3. **CVE ID : CVE-2021-28812**	https://www.qnap.com/zh-tw/security-advisory/qsa-21-21	O-QNA-QUTS-180621/693
quts_hero					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-21	3.5	A DOM-based XSS vulnerability has been reported to affect QNAP NAS running QTS and QuTS hero. If exploited, this vulnerability allows attackers to inject malicious code. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.3.1652 Build 20210428. QNAP Systems Inc. QuTS hero versions prior to h4.5.2.1638 Build 20210414. QNAP Systems Inc. QuTScloud versions prior to c4.5.5.1656 Build 20210503. This issue does not affect: QNAP Systems Inc. QTS 4.3.6; 4.3.3. **CVE ID : CVE-2021-28806**	https://www.qnap.com/zh-tw/security-advisory/qsa-21-22	O-QNA-QUTS-180621/694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-21	3.5	A post-authentication reflected XSS vulnerability has been reported to affect QNAP NAS running Q'center. If exploited, this vulnerability allows remote attackers to inject malicious code. QNAP have already fixed this vulnerability in the following versions of Q'center: QTS 4.5.3: Q'center v1.12.1012 and later QTS 4.3.6: Q'center v1.10.1004 and later QTS 4.3.3: Q'center v1.10.1004 and later QuTS hero h4.5.2: Q'center v1.12.1012 and later QuTScloud c4.5.4: Q'center v1.12.1012 and later **CVE ID : CVE-2021-28807**	https://www.qnap.com/zh-tw/security-advisory/qsa-21-20	O-QNA-QUTS-180621/695
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Jun-21	6.5	A command injection vulnerability has been reported to affect certain versions of Video Station. If exploited, this vulnerability allows remote attackers to execute arbitrary commands. This issue affects: QNAP Systems Inc. Video Station versions prior to 5.5.4 on QTS 4.5.2; versions prior to 5.5.4 on QuTS hero h4.5.2; versions prior to 5.5.4 on QuTScloud c4.5.4. This issue does not affect: QNAP Systems Inc. Video Station on QTS 4.3.6; on QTS 4.3.3. **CVE ID : CVE-2021-28812**	https://www.qnap.com/zh-tw/security-advisory/qsa-21-21	O-QNA-QUTS-180621/696
Redhat					
enterprise_linux					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jun-21	6.5	A flaw was found in postgresql in versions before 13.3, before 12.7, before 11.12, before 10.17 and before 9.6.22. While modifying certain SQL array values, missing bounds checks let authenticated database users write arbitrary bytes to a wide area of server memory. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-32027**	https://www.postgresql.org/support/security/CVE-2021-32027/, https://bugzilla.redhat.com/show_bug.cgi?id=1956876	O-RED-ENTE-180621/697
Use After Free	01-Jun-21	6.8	There's a flaw in libxml2's xmllint in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by xmllint could trigger a use-after-free. The greatest impact of this flaw is to confidentiality, integrity, and availability. **CVE ID : CVE-2021-3516**	https://gitlab.gnome.org/GNOME/libxml2/-/commit/1358d157d0bd83be1dfe356a69213df9fac0b539	O-RED-ENTE-180621/698
NULL Pointer Dereference	01-Jun-21	7.2	A flaw null pointer dereference in the Nitro Enclaves kernel driver was found in the way that Enclaves VMs forces closures on the enclave file descriptor. A local user of a host machine could use this flaw to crash the system or escalate their privileges on the system. **CVE ID : CVE-2021-3543**	N/A	O-RED-ENTE-180621/699
Exposure of Sensitive	04-Jun-21	4.3	A flaw was found in tpm2-tools in versions before 5.1.1	https://bugzilla.redhat.co	O-RED-ENTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information to an Unauthorized Actor			and before 4.3.2. tpm2_import used a fixed AES key for the inner wrapper, potentially allowing a MITM attacker to unwrap the inner portion and reveal the key being imported. The highest threat from this vulnerability is to data confidentiality. **CVE ID : CVE-2021-3565**	m/show_bug.cgi?id=1964427	180621/700
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Jun-21	2.1	A stack corruption bug was found in libtpms in versions before 0.7.2 and before 0.8.0 while decrypting data using RSA. This flaw could result in a SIGBUS (bad memory access) and termination of swtpm. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2021-3569**	https://bugzilla.redhat.com/show_bug.cgi?id=1964358	O-RED-ENTE-180621/701