Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Accellion					
fta					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-Mar-21	7.5	Accellion FTA 9_12_432 and earlier is affected by argument injection via a crafted POST request to an admin endpoint. The fixed version is FTA_9_12_444 and later. **CVE ID : CVE-2021-27730**	N/A	A-ACC-FTA-160321/1
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-21	4.3	Accellion FTA 9_12_432 and earlier is affected by stored XSS via a crafted POST request to a user endpoint. The fixed version is FTA_9_12_444 and later. **CVE ID : CVE-2021-27731**	N/A	A-ACC-FTA-160321/2
adguard					
adguard_home					
Improper Restriction of Excessive Authentication Attempts	03-Mar-21	5	An issue was discovered in AdGuard before 0.105.2. An attacker able to get the user's cookie is able to bruteforce their password offline, because the hash of the password is stored in the cookie. **CVE ID : CVE-2021-27935**	https://github.com/AdguardTeam/AdGuardHome/issues/2470	A-ADG-ADGU-160321/3
Afterlogic					
webmail_pro					
Improper	04-Mar-21	6.8	An issue was discovered in	https://auror	A-AFT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			AfterLogic Aurora through 8.5.3 and WebMail Pro through 8.5.3, when DAV is enabled. They allow directory traversal to create new files (such as an executable file under the web root). This is related to DAVServer.php in 8.x and DAV/Server.php in 7.x. **CVE ID : CVE-2021-26293**	amail.wordpress.com/2021/02/03/addressing-dav-related-vulnerability-in-webmail-and-aurora/	WEBM-160321/4
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Mar-21	5	An issue was discovered in AfterLogic Aurora through 7.7.9 and WebMail Pro through 7.7.9. They allow directory traversal to read files (such as a data/settings/settings.xml file containing admin panel credentials), as demonstrated by dav/server.php/files/personal/%2e%2e when using the caldav_public_user account (with caldav_public_user as its password). **CVE ID : CVE-2021-26294**	N/A	A-AFT-WEBM-160321/5
aurora					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Mar-21	6.8	An issue was discovered in AfterLogic Aurora through 8.5.3 and WebMail Pro through 8.5.3, when DAV is enabled. They allow directory traversal to create new files (such as an executable file under the web root). This is related to DAVServer.php in 8.x and	https://auroramail.wordpress.com/2021/02/03/addressing-dav-related-vulnerability-in-webmail-and-aurora/	A-AFT-AURO-160321/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DAV/Server.php in 7.x. **CVE ID : CVE-2021-26293**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Mar-21	5	An issue was discovered in AfterLogic Aurora through 7.7.9 and WebMail Pro through 7.7.9. They allow directory traversal to read files (such as a data/settings/settings.xml file containing admin panel credentials), as demonstrated by dav/server.php/files/personal/%2e%2e when using the caldav_public_user account (with caldav_public_user as its password). **CVE ID : CVE-2021-26294**	N/A	A-AFT-AURO-160321/7
ansi_up_project					
ansi_up					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Mar-21	4.3	The npm package ansi_up converts ANSI escape codes into HTML. In ansi_up v4, ANSI escape codes can be used to create HTML hyperlinks. Due to insufficient URL sanitization, this feature is affected by a cross-site scripting (XSS) vulnerability. This issue is fixed in v5.0.0. **CVE ID : CVE-2021-3377**	https://github.com/drudru/ansi_up/commit/c8c726ed1db979bae4f257b7fa41775155ba2e27	A-ANS-ANSI-160321/8
anuko					
time_tracker					
Use of Insufficiently	03-Mar-21	5	Anuko Time Tracker is an open source, web-based	https://github.com/anuko	A-ANU-TIME-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Random Values			time tracking application written in PHP. In TimeTracker before version 1.19.24.5415 tokens used in password reset feature in Time Tracker are based on system time and, therefore, are predictable. This opens a window for brute force attacks to guess user tokens and, once successful, change user passwords, including that of a system administrator. This vulnerability is pathced in version 1.19.24.5415 (started to use more secure tokens) with an additional improvement in 1.19.24.5416 (limited an available window for brute force token guessing). **CVE ID : CVE-2021-21352**	/timetracker/commit/40f3d9345adc20e6f28eb9f59e2489aff87fecf5, https://github.com/anuko/timetracker/security/advisories/GHSA-43c9-rx4h-4gqq, https://www.anuko.com/time-tracker/index.htm	160321/9
Apache					
tomcat					
Exposure of Sensitive Information to an Unauthorized Actor	01-Mar-21	5	When responding to new h2c connection requests, Apache Tomcat versions 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41 and 8.5.0 to 8.5.61 could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's	https://lists.apache.org/thread.html/r7b95bc248603360501f18c8eb03bb6001ec0ee3296205b34b07105b7%40%3Cannounce.tomcat.apache.org%3E, https://lists.a	A-APA-TOMC-160321/10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request. **CVE ID : CVE-2021-25122**	pache.org/thread.html/r7b95bc248603360501f18c8eb03bb6001ec0ee3296205b34b07105b7@%3Cannounce.apache.org%3E	
Not Available	01-Mar-21	4.4	The fix for CVE-2020-9484 was incomplete. When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue. **CVE ID : CVE-2021-25329**	https://lists.apache.org/thread.html/rf6d5d57b114678d8898005faef31e9fd6d7c981fcc4ccfc3bc272fc9@%3Cdev.tomcat.apache.org%3E, https://lists.apache.org/thread.html/rfe62fbf9d4c314f166fe8c668e50e5d9dd882a99447f26f0367474bf%40%3Cannounce.tomcat.apache.org%3E	A-APA-TOMC-160321/11
superset					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Mar-21	3.5	Apache Superset up to and including 0.38.0 allowed the creation of a Markdown component on a Dashboard page for describing chart's related information. Abusing this functionality,	https://lists.apache.org/thread.html/r09293fb09f1d617f0d2180c42210e739e2211f8da9bc5c	A-APA-SUPE-160321/12

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a malicious user could inject javascript code executing unwanted action in the context of the user's browser. The javascript code will be automatically executed (Stored XSS) when a legitimate user surfs on the dashboard page. The vulnerability is exploitable creating a “div” section and embedding in it a “svg” element with javascript code. **CVE ID : CVE-2021-27907**	1873bea67a%40%3Cdev.superset.apache.org%3E, https://lists.apache.org/thread.html/r09293fb09f1d617f0d2180c42210e739e2211f8da9bc5c1873bea67a@%3Cdev.superset.apache.org%3E	
Arubanetworks					
airwave					
Cross-Site Request Forgery (CSRF)	05-Mar-21	6.8	A remote unauthenticated cross-site request forgery (csrf) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the AirWave web-based management interface could allow an unauthenticated remote attacker to conduct a CSRF attack against a vulnerable system. A successful exploit would consist of an attacker persuading an authorized user to follow a malicious link, resulting in arbitrary actions being carried out with the privilege level of the targeted user.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-005.txt	A-ARU-AIRW-160321/13

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26960		
Cross-Site Request Forgery (CSRF)	05-Mar-21	6.8	A remote unauthenticated cross-site request forgery (csrf) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the AirWave web-based management interface could allow an unauthenticated remote attacker to conduct a CSRF attack against a vulnerable system. A successful exploit would consist of an attacker persuading an authorized user to follow a malicious link, resulting in arbitrary actions being carried out with the privilege level of the targeted user. **CVE ID : CVE-2021-26961**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-005.txt	A-ARU-AIRW-160321/14
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Mar-21	9	A remote authenticated arbitrary command execution vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Vulnerabilities in the AirWave CLI could allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-005.txt	A-ARU-AIRW-160321/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system leading to full system compromise. **CVE ID : CVE-2021-26962**		
Not Available	05-Mar-21	9	A remote authenticated arbitrary command execution vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Vulnerabilities in the AirWave CLI could allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to full system compromise. **CVE ID : CVE-2021-26963**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-005.txt	A-ARU-AIRW-160321/16
Incorrect Authorization	05-Mar-21	5.5	A remote authentication restriction bypass vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the AirWave web-based management interface could allow an authenticated remote attacker to improperly access and modify devices and management user details. A successful exploit would consist of an	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-005.txt	A-ARU-AIRW-160321/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker using a lower privileged account to change management user or device details. This could allow the attacker to escalate privileges and/or change network details that they should not have access to. **CVE ID : CVE-2021-26964**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Mar-21	5.5	A remote authenticated sql injection vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Multiple vulnerabilities in the API of AirWave could allow an authenticated remote attacker to conduct SQL injection attacks against the AirWave instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database. **CVE ID : CVE-2021-26965**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-005.txt	A-ARU-AIRW-160321/18
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Mar-21	5.5	A remote authenticated sql injection vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Multiple vulnerabilities in the API of AirWave could allow an authenticated remote attacker to conduct SQL injection attacks against the AirWave instance. An	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-005.txt	A-ARU-AIRW-160321/19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database. **CVE ID : CVE-2021-26966**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Mar-21	4.3	A remote reflected cross-site scripting (xss) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the web-based management interface of AirWave could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of certain components of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the AirWave management interface. **CVE ID : CVE-2021-26967**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-005.txt	A-ARU-AIRW-160321/20
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Mar-21	3.5	A remote authenticated stored cross-site scripting (xss) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the web-based management interface of AirWave could allow an authenticated remote	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-005.txt	A-ARU-AIRW-160321/21

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2021-26968**		
Improper Restriction of XML External Entity Reference	05-Mar-21	5.5	A remote authenticated authenticated xml external entity (xxe) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Due to improper restrictions on XML entities a vulnerability exists in the web-based management interface of AirWave. A successful exploit could allow an authenticated attacker to retrieve files from the local system or cause the application to consume system resources, resulting in a denial of service condition. **CVE ID : CVE-2021-26969**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-005.txt	A-ARU-AIRW-160321/22
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Mar-21	6.5	A remote authenticated arbitrary command execution vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Vulnerabilities in the AirWave web-base	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-005.txt	A-ARU-AIRW-160321/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface could allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as a lower privileged user on the underlying operating system leading to partial system compromise. **CVE ID : CVE-2021-26970**		
Not Available	05-Mar-21	6.5	A remote authenticated arbitrary command execution vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Vulnerabilities in the AirWave web-base management interface could allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as a lower privileged user on the underlying operating system leading to partial system compromise. **CVE ID : CVE-2021-26971**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-005.txt	A-ARU-AIRW-160321/24
bam_project					
bam					
Integer	05-Mar-21	7.5	An issue was discovered in	https://rusts	A-BAM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			the bam crate before 0.1.3 for Rust. There is an integer underflow and out-of-bounds write during the loading of a bgzip block. **CVE ID : CVE-2021-28027**	ec.org/advisories/RUSTSEC-2021-0027.html	BAM-160321/25
batflat					
batflat					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Mar-21	3.5	Cross-site scripting (XSS) vulnerability in Galleries in Batflat CMS 1.3.6 allows remote attackers to inject arbitrary web script or HTML via the field name. **CVE ID : CVE-2021-27677**	N/A	A-BAT-BATF-160321/26
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Mar-21	3.5	Cross-site scripting (XSS) vulnerability in Snippets in Batflat CMS 1.3.6 allows remote attackers to inject arbitrary web script or HTML via the field name. **CVE ID : CVE-2021-27678**	N/A	A-BAT-BATF-160321/27
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Mar-21	3.5	Cross-site scripting (XSS) vulnerability in Navigation in Batflat CMS 1.3.6 allows remote attackers to inject arbitrary web script or HTML via the field name. **CVE ID : CVE-2021-27679**	N/A	A-BAT-BATF-160321/28
bigprof					
online_invoicing_system					
Improper Neutralization of Formula Elements in a CSV File	03-Mar-21	5.8	A CSV injection vulnerability found in Online Invoicing System (OIS) 4.3 and below can be exploited by users to perform malicious actions	N/A	A-BIG-ONLI-160321/29

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			such as redirecting admins to unknown or harmful websites, or disclosing other clients' details that the user did not have access to. **CVE ID : CVE-2021-27839**		
byte_struct_project					
byte_struct					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Mar-21	7.5	An issue was discovered in the byte_struct crate before 0.6.1 for Rust. There can be a drop of uninitialized memory if a certain deserialization method panics. **CVE ID : CVE-2021-28033**	https://rustsec.org/advisories/RUSTSEC-2021-0032.html	A-BYT-BYTE-160321/30
cszcms					
csz_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Mar-21	3.5	A stored cross-site scripting (XSS) vulnerability in cszcms 1.2.9 exists in /admin/pages/new via the content parameter. **CVE ID : CVE-2021-3224**	N/A	A-CSZ-CSZ_-160321/31
datadoghq					
datadog-api-client-java					
Creation of Temporary File With Insecure Permissions	03-Mar-21	4.3	The Java client for the Datadog API before version 1.0.0-beta.9 has a local information disclosure of sensitive information downloaded via the API using the API Client. The Datadog API is executed on a unix-like system with	https://github.com/DataDog/datadog-api-client-java/releases/tag/datadog-api-client-1.0.0-beta.9, https://githu	A-DAT-DATA-160321/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple users. The API is used to download a file containing sensitive information. This sensitive information is exposed locally to other users. This vulnerability exists in the API Client for version 1 and 2. The method `prepareDownloadFilecreates` creates a temporary file with the permissions bits of `-rw-r--r--` on unix-like systems. On unix-like systems, the system temporary directory is shared between users. As such, the contents of the file downloaded via the `downloadFileFromResponse` method will be visible to all other users on the local system. Analysis of the finding determined that the affected code was unused, meaning that the exploitation likelihood is low. The unused code has been removed, effectively mitigating this issue. This issue has been patched in version 1.0.0-beta.9. As a workaround one may specify `java.io.tmpdir` when starting the JVM with the flag `-Djava.io.tmpdir`, specifying a path to a directory with `drw-------` permissions owned by `dd-agent`. **CVE ID : CVE-2021-21331**	b.com/DataDog/datadog-api-client-java/security/advisories/GHSA-2cxf-6567-7pp6	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dataiku					
data_science_studio					
Incorrect Authorization	01-Mar-21	5.5	In Dataiku DSS before 8.0.6, insufficient access control in the Jupyter notebooks integration allows users (who have coding permissions) to read and overwrite notebooks in projects that they are not authorized to access. **CVE ID : CVE-2021-27225**	https://doc.dataiku.com/dss/8.0/security/advisories/cve-2021-27225.html, https://doc.dataiku.com/dss/latest/	A-DAT-DATA-160321/33
Dell					
openmanage_server_administrator					
Improper Authentication	02-Mar-21	7.5	Dell EMC OpenManage Server Administrator (OMSA) version 9.5 Microsoft Windows installations with Distributed Web Server (DWS) enabled configuration contains an authentication bypass vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to gain admin access on the affected system. **CVE ID : CVE-2021-21513**	https://www.dell.com/support/kbdoc/en-us/000183670/dsa-2021-040-dell-emc-openmanage-server-administrator-omsa-security-update-for-multiple-vulnerabilities	A-DEL-OPEN-160321/34
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Mar-21	4	Dell EMC OpenManage Server Administrator (OMSA) versions 9.5 and prior contain a path traversal vulnerability. A remote user with admin privileges could potentially exploit this vulnerability to	https://www.dell.com/support/kbdoc/en-us/000183670/dsa-2021-040-dell-emc-openmanage-	A-DEL-OPEN-160321/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			view arbitrary files on the target system by sending a specially crafted URL request. **CVE ID : CVE-2021-21514**	server-administrator-omsa-security-update-for-multiple-vulnerabilities	
emc_sourceone					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-21	3.5	Dell EMC SourceOne, versions 7.2SP10 and prior, contain a Stored Cross-Site Scripting vulnerability. A remote low privileged attacker may potentially exploit this vulnerability, to hijack user sessions or to trick a victim application user to unknowingly send arbitrary requests to the server. **CVE ID : CVE-2021-21515**	https://www.dell.com/support/kbdoc/en-us/000183430/dsa-2021-043-dell-emc-sourceone-java-script-xss-stored-vulnerability	A-DEL-EMC_-160321/36
emc_srs_policy_manager					
Improper Restriction of XML External Entity Reference	01-Mar-21	6.4	SRS Policy Manager 6.X is affected by an XML External Entity Injection (XXE) vulnerability due to a misconfigured XML parser that processes user-supplied DTD input without sufficient validation. A remote unauthenticated attacker can potentially exploit this vulnerability to read system files as a non-root user and may be able to temporarily disrupt the ESRS service.	https://www.dell.com/support/kbdoc/en-us/000183576/dsa-2021-045-dell-emc-srs-policy-manager-security-update-for-external-entity-injection-vulnerability	A-DEL-EMC_-160321/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21517		
deutschepost					
mailoptimizer					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Mar-21	8.3	Deutsche Post Mailoptimizer 4.3 before 2020-11-09 allows Directory Traversal via a crafted ZIP archive to the Upload feature or the MO Connect component. This can lead to remote code execution. **CVE ID : CVE-2021-28042**	N/A	A-DEU-MAIL-160321/38
docker_dashboard_project					
docker_dashboard					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Mar-21	7.5	rakibtg Docker Dashboard before 2021-02-28 allows command injection in backend/utilities/terminal.js via shell metacharacters in the command parameter of an API request. NOTE: this is NOT a Docker, Inc. product. **CVE ID : CVE-2021-27886**	https://github.com/rakibtg/docker-web-gui/commit/79cdc41809f2030fce21a1109898bd79e4190661	A-DOC-DOCK-160321/39
doctor_appointment_system_project					
doctor_appointment_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Mar-21	7.5	SQL injection in admin.php in doctor appointment system 1.0 allows an unauthenticated attacker to insert malicious SQL queries via username parameter at login page. **CVE ID : CVE-2021-27314**	N/A	A-DOC-DOCT-160321/40
Improper Neutralization	01-Mar-21	4.3	Cross Site Scripting (XSS) vulnerability in	N/A	A-DOC-DOCT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			contactus.php in Doctor Appointment System 1.0 allows remote attackers to inject arbitrary web script or HTML via the comment parameter. **CVE ID : CVE-2021-27317**		160321/41
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-21	4.3	Cross Site Scripting (XSS) vulnerability in contactus.php in Doctor Appointment System 1.0 allows remote attackers to inject arbitrary web script or HTML via the lastname parameter. **CVE ID : CVE-2021-27318**	N/A	A-DOC-DOCT-160321/42
Elastic					
elasticsearch					
Exposure of Sensitive Information to an Unauthorized Actor	08-Mar-21	4	A document disclosure flaw was found in Elasticsearch versions after 7.6.0 and before 7.11.0 when Document or Field Level Security is used. Get requests do not properly apply security permissions when executing a query against a recently updated document. This affects documents that have been updated and not yet refreshed in the index. This could result in the search disclosing the existence of documents and fields the attacker should not be able to view. **CVE ID : CVE-2021-22134**	https://discuss.elastic.co/t/elastic-stack-7-11-0-security-update/265835	A-ELA-ELAS-160321/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
eprints					
eprints					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Mar-21	6.8	EPrints 3.4.2 allows remote attackers to read arbitrary files and possibly execute commands via crafted LaTeX input to a cgi/latex2png?latex= URI. **CVE ID : CVE-2021-3342**	https://files.eprints.org/2548/, https://files.eprints.org/2549/, https://github.com/grymer/CVE/blob/master/eprints_security_review.pdf	A-EPR-EPRI-160321/44
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-21	4.3	EPrints 3.4.2 exposes a reflected XSS opportunity in the via a cgi/cal URI. **CVE ID : CVE-2021-26475**	https://files.eprints.org/2548/, https://github.com/grymer/CVE/blob/master/eprints_security_review.pdf	A-EPR-EPRI-160321/45
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Mar-21	7.5	EPrints 3.4.2 allows remote attackers to execute OS commands via crafted LaTeX input to a cgi/cal?year= URI. **CVE ID : CVE-2021-26476**	https://files.eprints.org/2548/, https://github.com/grymer/CVE/blob/master/eprints_security_review.pdf	A-EPR-EPRI-160321/46
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-21	4.3	EPrints 3.4.2 exposes a reflected XSS opportunity in the dataset parameter to the cgi/dataset_dictionary URI. **CVE ID : CVE-2021-26702**	https://files.eprints.org/2548/, https://github.com/grymer/CVE/blob/master/eprin	A-EPR-EPRI-160321/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ts_security_review.pdf	
Improper Restriction of XML External Entity Reference	01-Mar-21	7.5	EPrints 3.4.2 allows remote attackers to read arbitrary files and possibly execute commands via crafted JSON/XML input to a cgi/ajax/phrase URI. **CVE ID : CVE-2021-26703**	https://files.eprints.org/2548/, https://files.eprints.org/2549/, https://github.com/grymer/CVE/blob/master/eprints_security_review.pdf	A-EPR-EPRI-160321/48
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Mar-21	6.5	EPrints 3.4.2 allows remote attackers to execute arbitrary commands via crafted input to the verb parameter in a cgi/toolbox/toolbox URI. **CVE ID : CVE-2021-26704**	https://files.eprints.org/2548/, https://files.eprints.org/2549/, https://github.com/grymer/CVE/blob/master/eprints_security_review.pdf	A-EPR-EPRI-160321/49
Facebook					
zstandard					
Incorrect Default Permissions	04-Mar-21	6.4	In the Zstandard command-line utility prior to v1.4.1, output files were created with default permissions. Correct file permissions (matching the input) would only be set at completion time. Output files could therefore be readable or writable to unintended parties.	https://www.facebook.com/security/advisories/cve-2021-24031	A-FAC-ZSTA-160321/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24031		
Incorrect Default Permissions	04-Mar-21	6.4	Beginning in v1.4.1 and prior to v1.4.9, due to an incomplete fix for CVE-2021-24031, the Zstandard command-line utility created output files with default permissions and restricted those permissions immediately afterwards. Output files could therefore momentarily be readable or writable to unintended parties. **CVE ID : CVE-2021-24032**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=982519, https://github.com/facebook/zstd/issues/2491	A-FAC-ZSTA-160321/51
react-dev-utils					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Mar-21	6.8	react-dev-utils prior to v11.0.4 exposes a function, getProcessForPort, where an input argument is concatenated into a command string to be executed. This function is typically used from react-scripts (in Create React App projects), where the usage is safe. Only when this function is manually invoked with user-provided values (ie: by custom code) is there the potential for command injection. If you're consuming it from react-scripts then this issue does not affect you. **CVE ID : CVE-2021-24033**	https://github.com/facebook/create-react-app/pull/10644, https://www.facebook.com/security/advisories/cve-2021-24033	A-FAC-REAC-160321/52
fastify-http-proxy_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fastify-http-proxy					
Improper Input Validation	02-Mar-21	7.5	fastify-http-proxy is an npm package which is a fastify plugin for proxying your http requests to another server, with hooks. By crafting a specific URL, it is possible to escape the prefix of the proxied backend service. If the base url of the proxied server is `/pub/`, a user expect that accessing `/priv` on the target service would not be possible. In affected versions, it is possible. This is fixed in version 4.3.1. **CVE ID : CVE-2021-21322**	https://github.com/fastify/fastify-http-proxy/commit/02d9b43c770aa16bc44470edecfaeb7c17985016, https://github.com/fastify/fastify-http-proxy/security/advisories/GHSA-c4qr-gmr9-v23w	A-FAS-FAST-160321/53
fastify-reply-from_project					
fastify-reply-from					
Improper Input Validation	02-Mar-21	7.5	fastify-reply-from is an npm package which is a fastify plugin to forward the current http request to another server. In fastify-reply-from before version 4.0.2, by crafting a specific URL, it is possible to escape the prefix of the proxied backend service. If the base url of the proxied server is "/pub/", a user expect that accessing "/priv" on the target service would not be possible. In affected versions, it is possible. This is fixed in version 4.0.2. **CVE ID : CVE-2021-21321**	https://github.com/fastify/fastify-reply-from/commit/dea227dda606900cc01870d08541b4dcc69d3889, https://github.com/fastify/fastify-reply-from/security/advisories/GHSA-qmw8-3v4g-gwj4	A-FAS-FAST-160321/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Fatek					
fvdesigner					
Out-of-bounds Read	03-Mar-21	6.8	Fatek FvDesigner Version 1.5.76 and prior is vulnerable to an out-of-bounds read while processing project files, allowing an attacker to craft a special project file that may permit arbitrary code execution. **CVE ID : CVE-2021-22638**	N/A	A-FAT-FVDE-160321/55
Use After Free	03-Mar-21	6.8	A use after free issue has been identified in Fatek FvDesigner Version 1.5.76 and prior in the way the application processes project files, allowing an attacker to craft a special project file that may permit arbitrary code execution. **CVE ID : CVE-2021-22662**	N/A	A-FAT-FVDE-160321/56
Out-of-bounds Write	03-Mar-21	6.8	Fatek FvDesigner Version 1.5.76 and prior is vulnerable to a stack-based buffer overflow while project files are being processed, allowing an attacker to craft a special project file that may permit arbitrary code execution. **CVE ID : CVE-2021-22666**	N/A	A-FAT-FVDE-160321/57
Access of Uninitialized Pointer	03-Mar-21	6.8	An uninitialized pointer may be exploited in Fatek FvDesigner Version 1.5.76 and prior while the application is processing project files, allowing an	N/A	A-FAT-FVDE-160321/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to craft a special project file that may permit arbitrary code execution. **CVE ID : CVE-2021-22670**		
Out-of-bounds Write	03-Mar-21	6.8	Fatek FvDesigner Version 1.5.76 and prior is vulnerable to an out-of-bounds write while processing project files, allowing an attacker to craft a special project file that may permit arbitrary code execution. **CVE ID : CVE-2021-22683**	N/A	A-FAT-FVDE-160321/59
fireblink					
object-collider					
Not Available	01-Mar-21	7.5	Prototype pollution vulnerability in 'object-collider' versions 1.0.0 through 1.0.3 allows attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2021-25914**	https://github.com/FireBlinkLTD/object-collider/commit/321f75a7f8e7b3393e5b7dd6dd9ab26ede5906e5	A-FIR-OBJE-160321/60
Fortinet					
fortiproxy					
Incorrect Authorization	04-Mar-21	4	An improper access control vulnerability in FortiProxy SSL VPN portal 2.0.0, 1.2.9 and below versions may allow an authenticated, remote attacker to access internal service such as the ZebOS Shell on the FortiProxy appliance through the Quick Connection functionality.	https://fortiguard.com/advisory/FG-IR-20-235	A-FOR-FORT-160321/61

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22128		
Github					
github					
Incorrect Authorization	03-Mar-21	4	An improper access control vulnerability was identified in GitHub Enterprise Server that allowed authenticated users of the instance to gain write access to unauthorized repositories via specifically crafted pull requests and REST API requests. An attacker would need to be able to fork the targeted repository, a setting that is disabled by default for organization owned private repositories. Branch protections such as required pull request reviews or status checks would prevent unauthorized commits from being merged without further review or validation. This vulnerability affected all versions of GitHub Enterprise Server since 2.4.21 and was fixed in versions 2.20.24, 2.21.15, 2.22.7 and 3.0.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2021-22861**	https://docs.github.com/en/enterprise-server@2.20/admin/release-notes#2.20.24, https://docs.github.com/en/enterprise-server@2.21/admin/release-notes#2.21.15, https://docs.github.com/en/enterprise-server@2.22/admin/release-notes#2.22.7	A-GIT-GITH-160321/62
Incorrect Authorization	03-Mar-21	4	An improper access control vulnerability was identified	https://docs.github.com/e	A-GIT-GITH-160321/63

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in GitHub Enterprise Server that allowed an authenticated user with the ability to fork a repository to disclose Actions secrets for the parent repository of the fork. This vulnerability existed due to a flaw that allowed the base reference of a pull request to be updated to point to an arbitrary SHA or another pull request outside of the fork repository. By establishing this incorrect reference in a PR, the restrictions that limit the Actions secrets sent a workflow from forks could be bypassed. This vulnerability affected GitHub Enterprise Server version 3.0.0, 3.0.0.rc2, and 3.0.0.rc1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2021-22862**	n/enterprise-server@3.0/admin/release-notes#3.0.1	
Incorrect Authorization	03-Mar-21	5.5	An improper access control vulnerability was identified in the GitHub Enterprise Server GraphQL API that allowed authenticated users of the instance to modify the maintainer collaboration permission of a pull request without proper authorization. By exploiting this vulnerability, an attacker	https://docs.github.com/en/enterprise-server@2.20/admin/release-notes#2.20.24, https://docs.github.com/en/enterprise-server@2.21/	A-GIT-GITH-160321/64

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would be able to gain access to head branches of pull requests opened on repositories of which they are a maintainer. Forking is disabled by default for organization owned private repositories and would prevent this vulnerability. Additionally, branch protections such as required pull request reviews or status checks would prevent unauthorized commits from being merged without further review or validation. This vulnerability affected all versions of GitHub Enterprise Server since 2.12.22 and was fixed in versions 2.20.24, 2.21.15, 2.22.7 and 3.0.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2021-22863**	admin/release-notes#2.21.15, https://docs.github.com/en/enterprise-server@2.22/admin/release-notes#2.22.7	
Gitlab					
gitlab					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-21	3.5	An issue has been discovered in GitLab affecting all versions starting with 13.7. GitLab was vulnerable to a stored XSS in merge request. **CVE ID : CVE-2021-22182**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22182.json	A-GIT-GITL-160321/65
Improper Neutralization	04-Mar-21	3.5	An issue has been discovered in GitLab	https://gitlab.com/gitlab-	A-GIT-GITL-160321/66

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			affecting all versions starting with 11.8. GitLab was vulnerable to a stored XSS in the epics page, which could be exploited with user interactions. **CVE ID : CVE-2021-22183**	org/cves/-/blob/master/2021/CVE-2021-22183.json	
Uncontrolled Resource Consumption	02-Mar-21	4	An issue has been discovered in GitLab affecting all versions of Gitlab EE/CE before 12.6.7. A potential resource exhaustion issue that allowed running or pending jobs to continue even after project was deleted. **CVE ID : CVE-2021-22187**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22187.json	A-GIT-GITL-160321/67
Not Available	03-Mar-21	5	An issue has been discovered in GitLab affecting all versions starting with 13.0. Confidential issue titles in Gitlab were readable by an unauthorised user via branch logs. **CVE ID : CVE-2021-22188**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22188.json	A-GIT-GITL-160321/68
Improper Certificate Validation	04-Mar-21	6.5	Starting with version 13.7 the Gitlab CE/EE editions were affected by a security issue related to the validation of the certificates for the Fortinet OTP that could result in authentication issues. **CVE ID : CVE-2021-22189**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22189.json	A-GIT-GITL-160321/69
Glpi-project					
glpi					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	02-Mar-21	3.5	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. In GLPI version 9.5.3, it was possible to switch entities with IDOR from a logged in user. This is fixed in version 9.5.4. **CVE ID : CVE-2021-21255**	https://github.com/glpi-project/glpi/commit/aade65b7f67d46f23d276a8acb0df70651c3b1dc, https://github.com/glpi-project/glpi/security/advisories/GHSA-v3m5-r3mx-ff9j	A-GLP-GLPI-160321/70
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-21	3.5	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. In GLPI from version 9.5.0 and before version 9.5.4, there is a cross-site scripting injection vulnerability when using ajax/kanban.php. This is fixed in version 9.5.4. **CVE ID : CVE-2021-21258**	https://github.com/glpi-project/glpi/commit/e7802fc051696de1f76108ea8dc3bd4e2c880f15, https://github.com/glpi-project/glpi/security/advisories/GHSA-j4xj-4qmc-mmmx	A-GLP-GLPI-160321/71
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-21	3.5	GLPI is open source software which stands for Gestionnaire Libre de Parc Informatique and it is a Free Asset and IT Management Software package. In GLPI before verison 9.5.4, there is a vulnerability within the document upload function	https://github.com/glpi-project/glpi/security/advisories/GHSA-c7f6-3mr7-3rq2	A-GLP-GLPI-160321/72

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Home > Management > Documents > Add, or /front/document.form.php endpoint), indeed one of the form field: "Web Link" is not properly sanitized and a malicious user (who has document upload rights) can use it to deliver JavaScript payload. For example if you use the following payload: " accesskey="x" onclick="alert(1)" x=", the content will be saved within the database without any control. And then once you return to the summary documents page, by clicking on the "Web Link" of the newly created file it will create a new empty tab, but on the initial tab the pop-up "1" will appear. **CVE ID : CVE-2021-21312**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Mar-21	4	GLPI is open source software which stands for Gestionnaire Libre de Parc Informatique and it is a Free Asset and IT Management Software package. In GLPI before verison 9.5.4, there is a vulnerability in the /ajax/common.tabs.php endpoint, indeed, at least two parameters _target and id are not properly sanitized. Here are two	https://github.com/glpi-project/glpi/security/advisories/GHSA-h4hj-mrpg-xfgx	A-GLP-GLPI-160321/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			payloads (due to two different exploitations depending on which parameter you act) to exploit the vulnerability:/ajax/common.tabs.php?_target=javascript:alert(document.cookie)&_itemtype=DisplayPreference&_glpi_tab=DisplayPreference$2&id=258&displaytype=Ticket (Payload triggered if you click on the button). /ajax/common.tabs.php?_target=/front/ticket.form.php&_itemtype=Ticket&_glpi_tab=Ticket$1&id=(){};(function%20(){alert(document.cookie);})();function%20a&#. **CVE ID : CVE-2021-21313**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-21	3.5	GLPI is open source software which stands for Gestionnaire Libre de Parc Informatique and it is a Free Asset and IT Management Software package. In GLPI before verison 9.5.4, there is an XSS vulnerability involving a logged in user while updating a ticket. **CVE ID : CVE-2021-21314**	https://github.com/glpi-project/glpi/security/advisories/GHSA-2w7j-xgj7-3xgg	A-GLP-GLPI-160321/74
GNU					
grub2					
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06. The option parser allows	N/A	A-GNU-GRUB-160321/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-20225**		
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-20233**	https://bugzilla.redhat.com/show_bug.cgi?id=1926263	A-GNU-GRUB-160321/76
Google					
chrome					
Out-of-bounds Write	09-Mar-21	6.8	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap	https://chromereleases.googleblog.com/2021/03/stable-	A-GOO-CHRO-160321/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption via a crafted HTML page. **CVE ID : CVE-2021-21159**	channel-update-for-desktop.html	
Out-of-bounds Write	09-Mar-21	6.8	Heap buffer overflow in WebAudio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21160**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/78
Out-of-bounds Write	09-Mar-21	6.8	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21161**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/79
Use After Free	09-Mar-21	6.8	Use after free in WebRTC in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21162**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/80
Origin Validation Error	09-Mar-21	4.3	Insufficient data validation in Reader Mode in Google Chrome on iOS prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page and a malicious server. **CVE ID : CVE-2021-21163**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/81
Origin	09-Mar-21	4.3	Insufficient data validation	https://chro	A-GOO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation Error			in Chrome on iOS in Google Chrome on iOS prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-21164**	mereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	CHRO-160321/82
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-21	6.8	Data race in audio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21165**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/83
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-21	6.8	Data race in audio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21166**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/84
Use After Free	09-Mar-21	6.8	Use after free in bookmarks in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21167**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/85
Not Available	09-Mar-21	4.3	Insufficient policy enforcement in appcache in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-	A-GOO-CHRO-160321/86

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTML page. **CVE ID : CVE-2021-21168**	desktop.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-21	6.8	Out of bounds memory access in V8 in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. **CVE ID : CVE-2021-21169**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/87
Not Available	09-Mar-21	4.3	Incorrect security UI in Loader in Google Chrome prior to 89.0.4389.72 allowed a remote attacker who had compromised the renderer process to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-21170**	N/A	A-GOO-CHRO-160321/88
Not Available	09-Mar-21	4.3	Incorrect security UI in TabStrip and Navigation in Google Chrome on Android prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-21171**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/89
Not Available	09-Mar-21	5.8	Insufficient policy enforcement in File System API in Google Chrome on Windows prior to 89.0.4389.72 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/90

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21172		
Not Available	09-Mar-21	4.3	Side-channel information leakage in Network Internals in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-21173**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/91
Use of Uninitialized Resource	09-Mar-21	6.8	Uninitialized data in PDFium in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file. **CVE ID : CVE-2021-21190**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/92
Not Available	09-Mar-21	6.8	Inappropriate implementation in Referrer in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2021-21174**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/93
Origin Validation Error	09-Mar-21	4.3	Inappropriate implementation in Site isolation in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-21175**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/94
Not Available	09-Mar-21	4.3	Inappropriate implementation in full screen mode in Google Chrome prior to	https://chromereleases.googleblog.com/2021/03/	A-GOO-CHRO-160321/95

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-21176**	stable-channel-update-for-desktop.html	
Improper Authentication	09-Mar-21	4.3	Insufficient policy enforcement in Autofill in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. **CVE ID : CVE-2021-21177**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/96
Not Available	09-Mar-21	4.3	Inappropriate implementation in Compositing in Google Chrome on Linux and Windows prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-21178**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/97
Use After Free	09-Mar-21	6.8	Use after free in Network Internals in Google Chrome on Linux prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21179**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/98
Use After Free	09-Mar-21	6.8	Use after free in tab search in Google Chrome prior to 89.0.4389.72 allowed a	https://chromereleases.googleblog.co	A-GOO-CHRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21180**	m/2021/03/stable-channel-update-for-desktop.html	160321/99
Not Available	09-Mar-21	4.3	Side-channel information leakage in autofill in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. **CVE ID : CVE-2021-21181**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/100
Incorrect Authorization	09-Mar-21	4.3	Insufficient policy enforcement in navigations in Google Chrome prior to 89.0.4389.72 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2021-21182**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/101
Origin Validation Error	09-Mar-21	4.3	Inappropriate implementation in performance APIs in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-21183**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/102
Origin Validation Error	09-Mar-21	4.3	Inappropriate implementation in performance APIs in Google Chrome prior to 89.0.4389.72 allowed a	https://chromereleases.googleblog.com/2021/03/stable-	A-GOO-CHRO-160321/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-21184**	channel-update-for-desktop.html	
Not Available	09-Mar-21	4.3	Insufficient policy enforcement in extensions in Google Chrome prior to 89.0.4389.72 allowed an attacker who convinced a user to install a malicious extension to obtain sensitive information via a crafted Chrome Extension. **CVE ID : CVE-2021-21185**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/104
Incorrect Authorization	09-Mar-21	4.3	Insufficient policy enforcement in QR scanning in Google Chrome on iOS prior to 89.0.4389.72 allowed an attacker who convinced the user to scan a QR code to bypass navigation restrictions via a crafted QR code. **CVE ID : CVE-2021-21186**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/105
Not Available	09-Mar-21	4.3	Insufficient data validation in URL formatting in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. **CVE ID : CVE-2021-21187**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/106
Use After Free	09-Mar-21	6.8	Use after free in Blink in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap	https://chromereleases.googleblog.com/2021/03/stable-	A-GOO-CHRO-160321/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption via a crafted HTML page. **CVE ID : CVE-2021-21188**	channel-update-for-desktop.html	
Improper Authentication	09-Mar-21	4.3	Insufficient policy enforcement in payments in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2021-21189**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	A-GOO-CHRO-160321/108
go-proxyproto_project					
go-proxyproto					
Not Available	08-Mar-21	4	The package github.com/pires/go-proxyproto before 0.5.0 are vulnerable to Denial of Service (DoS) via the parseVersion1() function. The reader in this package is a default bufio.Reader wrapping a net.Conn. It will read from the connection until it finds a newline. Since no limits are implemented in the code, a deliberately malformed V1 header could be used to exhaust memory in a server process using this code - and create a DoS. This can be exploited by sending a stream starting with PROXY and continuing to send data (which does not contain a newline) until the target stops acknowledging. The risk here is small, because only	https://github.com/pires/go-proxyproto/commit/7f48261db810703d173f27f3309a808cc2b49b8b, https://github.com/pires/go-proxyproto/pull/71	A-GO--GO-P-160321/109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			trusted sources should be allowed to send proxy protocol headers. **CVE ID : CVE-2021-23351**		
html-parse-stringify_project					
html-parse-stringify					
Not Available	04-Mar-21	5	This affects the package html-parse-stringify before 2.0.1; all versions of package html-parse-stringify2. Sending certain input could cause one of the regular expressions that is used for parsing to backtrack, freezing the process. **CVE ID : CVE-2021-23346**	https://github.com/HenrikJoreteg/html-parse-stringify/blob/master/lib/parse.js%23L2, https://github.com/HenrikJoreteg/html-parse-stringify/commit/c7274a48e59c92b2b7e906fedf9065159e73fe12, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1080633	A-HTM-HTML-160321/110
IBM					
rational_team_concert					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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://exchange.xforce.ibmcloud.com/vulnerabilities/194451, https://www.ibm.com/support/pages/n	A-IBM-RATI-160321/111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials disclosure within a trusted session. IBM X-Force ID: 194451. **CVE ID : CVE-2021-20340**	ode/6417585	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194707. **CVE ID : CVE-2021-20350**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194707, https://www.ibm.com/support/pages/node/6417585	A-IBM-RATI-160321/112
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194708. **CVE ID : CVE-2021-20351**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194708, https://www.ibm.com/support/pages/node/6417585	A-IBM-RATI-160321/113
engineering_lifecycle_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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.	https://exchange.xforce.ibmcloud.com/vulnerabilities/194451, https://www.ibm.com/support/pages/node/6417585	A-IBM-ENGI-160321/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 194451. **CVE ID : CVE-2021-20340**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194707. **CVE ID : CVE-2021-20350**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194707, https://www.ibm.com/support/pages/node/6417585	A-IBM-ENGI-160321/115
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194708. **CVE ID : CVE-2021-20351**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194708, https://www.ibm.com/support/pages/node/6417585	A-IBM-ENGI-160321/116
global_configuration_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194451.	https://exchange.xforce.ibmcloud.com/vulnerabilities/194451, https://www.ibm.com/support/pages/node/6417585	A-IBM-GLOB-160321/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20340		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194707. **CVE ID : CVE-2021-20350**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194707, https://www.ibm.com/support/pages/node/6417585	A-IBM-GLOB-160321/118
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194708. **CVE ID : CVE-2021-20351**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194708, https://www.ibm.com/support/pages/node/6417585	A-IBM-GLOB-160321/119
doors_next					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194451. **CVE ID : CVE-2021-20340**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194451, https://www.ibm.com/support/pages/node/6417585	A-IBM-DOOR-160321/120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194707. **CVE ID : CVE-2021-20350**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194707, https://www.ibm.com/support/pages/node/6417585	A-IBM-DOOR-160321/121
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194708. **CVE ID : CVE-2021-20351**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194708, https://www.ibm.com/support/pages/node/6417585	A-IBM-DOOR-160321/122
rational_doors_next_generation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194451. **CVE ID : CVE-2021-20340**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194451, https://www.ibm.com/support/pages/node/6417585	A-IBM-RATI-160321/123
Improper Neutralization	04-Mar-21	3.5	IBM Engineering products are vulnerable to cross-site	https://exchange.xforce.ib	A-IBM-RATI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			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: 194707. **CVE ID : CVE-2021-20350**	mcloud.com/vulnerabilities/194707, https://www.ibm.com/support/pages/node/6417585	160321/124
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194708. **CVE ID : CVE-2021-20351**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194708, https://www.ibm.com/support/pages/node/6417585	A-IBM-RATI-160321/125
rational_quality_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194451. **CVE ID : CVE-2021-20340**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194451, https://www.ibm.com/support/pages/node/6417585	A-IBM-RATI-160321/126
Improper Neutralization of Input During Web Page	04-Mar-21	3.5	IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed	https://exchange.xforce.ibmcloud.com/vulnerabilitie	A-IBM-RATI-160321/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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: 194707. **CVE ID : CVE-2021-20350**	s/194707, https://www.ibm.com/support/pages/node/6417585	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194708. **CVE ID : CVE-2021-20351**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194708, https://www.ibm.com/support/pages/node/6417585	A-IBM-RATI-160321/128
engineering_test_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194451. **CVE ID : CVE-2021-20340**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194451, https://www.ibm.com/support/pages/node/6417585	A-IBM-ENGI-160321/129
Improper Neutralization of Input During Web Page Generation ('Cross-site	04-Mar-21	3.5	IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering	https://exchange.xforce.ibmcloud.com/vulnerabilities/194707, https://www.	A-IBM-ENGI-160321/130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194707. **CVE ID : CVE-2021-20350**	ibm.com/support/pages/node/6417585	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194708. **CVE ID : CVE-2021-20351**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194708, https://www.ibm.com/support/pages/node/6417585	A-IBM-ENGI-160321/131
engineering_workflow_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194451. **CVE ID : CVE-2021-20340**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194451, https://www.ibm.com/support/pages/node/6417585	A-IBM-ENGI-160321/132
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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://exchange.xforce.ibmcloud.com/vulnerabilities/194707, https://www.ibm.com/support/pages/n	A-IBM-ENGI-160321/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials disclosure within a trusted session. IBM X-Force ID: 194707. **CVE ID : CVE-2021-20350**	ode/6417585	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194708. **CVE ID : CVE-2021-20351**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194708, https://www.ibm.com/support/pages/node/6417585	A-IBM-ENGI-160321/134
engineering_requirements_quality_assistant_on-premises					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194451. **CVE ID : CVE-2021-20340**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194451, https://www.ibm.com/support/pages/node/6417585	A-IBM-ENGI-160321/135
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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.	https://exchange.xforce.ibmcloud.com/vulnerabilities/194707, https://www.ibm.com/support/pages/node/6417585	A-IBM-ENGI-160321/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 194707. **CVE ID : CVE-2021-20350**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	3.5	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: 194708. **CVE ID : CVE-2021-20351**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194708, https://www.ibm.com/support/pages/node/6417585	A-IBM-ENGI-160321/137
cloud_pak_for_multicloud_management_monitoring					
Not Available	09-Mar-21	5	IBM Cloud Pak for Multicloud Management Monitoring 2.2 returns potentially sensitive information in headers which could lead to further attacks against the system. IBM X-Force ID: 194513. **CVE ID : CVE-2021-20341**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194513, https://www.ibm.com/support/pages/node/6426997	A-IBM-CLOU-160321/138
security_verify_bridge					
Use of a Broken or Risky Cryptographic Algorithm	03-Mar-21	4.3	IBM Security Verify Bridge uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 196617. **CVE ID : CVE-2021-20441**	https://exchange.xforce.ibmcloud.com/vulnerabilities/196617, https://www.ibm.com/support/pages/node/6421023	A-IBM-SECU-160321/139
Use of Hard-coded Credentials	03-Mar-21	5	IBM Security Verify Bridge contains hard-coded credentials, such as a password or cryptographic	https://exchange.xforce.ibmcloud.com/vulnerabilitie	A-IBM-SECU-160321/140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 196618. **CVE ID : CVE-2021-20442**	s/196618, https://www.ibm.com/support/pages/node/6421025	
Imagemagick					
imagemagick					
Divide By Zero	09-Mar-21	4.3	A flaw was found in ImageMagick in coders/jp2.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2021-20241**	https://github.com/ImageMagick/ImageMagick/pull/3177	A-IMA-IMAG-160321/141
Divide By Zero	09-Mar-21	4.3	A flaw was found in ImageMagick in MagickCore/resize.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2021-20243**	https://github.com/ImageMagick/ImageMagick/pull/3193	A-IMA-IMAG-160321/142
Impresscms					
impresscms					
Improper	11-Mar-21	3.5	Cross-site scripting (XSS) in	N/A	A-IMP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			modules/content/admin/content.php in ImpressCMS profile 1.4.2 allows remote attackers to inject arbitrary web script or HTML parameters through the "Display Name" field. **CVE ID : CVE-2021-28088**		IMPR-160321/143
internment_project					
internment					
Not Available	05-Mar-21	7.5	An issue was discovered in the internment crate before 0.4.2 for Rust. There is a data race that can cause memory corruption because of the unconditional implementation of Sync for Intern<T>. **CVE ID : CVE-2021-28037**	https://rustsec.org/advisories/RUSTSEC-2021-0036.html	A-INT-INTE-160321/144
Joomla					
joomla\!					
Inadequate Encryption Strength	04-Mar-21	5	An issue was discovered in Joomla! 3.2.0 through 3.9.24. Usage of the insecure rand() function within the process of generating the 2FA secret. **CVE ID : CVE-2021-23126**	https://developer.joomla.org/security-centre/841-20210301-core-insecure-randomness-within-2fa-secret-generation.html	A-JOO-JOOM-160321/145
Not Available	04-Mar-21	6.4	An issue was discovered in Joomla! 3.2.0 through 3.9.24. Usage of an insufficient length for the	https://developer.joomla.org/security-centre/841-	A-JOO-JOOM-160321/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2FA secret accoring to RFC 4226 of 10 bytes vs 20 bytes. **CVE ID : CVE-2021-23127**	20210301-core-insecure-randomness-within-2fa-secret-generation.html	
Not Available	04-Mar-21	6.4	An issue was discovered in Joomla! 3.2.0 through 3.9.24. The core shipped but unused randval implementation within FOF (FOFEncryptRandval) used an potential insecure implemetation. That has now been replaced with a call to 'random_bytes()' and its backport that is shipped within random_compat. **CVE ID : CVE-2021-23128**	https://developer.joomla.org/security-centre/842-20210302-core-potential-insecure-fofencryptrandval.html	A-JOO-JOOM-160321/147
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	4.3	An issue was discovered in Joomla! 2.5.0 through 3.9.24. Missing filtering of messages showed to users that could lead to xss issues. **CVE ID : CVE-2021-23129**	https://developer.joomla.org/security-centre/843-20210303-core-xss-within-alert-messages-showed-to-users.html	A-JOO-JOOM-160321/148
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-21	4.3	An issue was discovered in Joomla! 2.5.0 through 3.9.24. Missing filtering of feed fields could lead to xss issues. **CVE ID : CVE-2021-23130**	https://developer.joomla.org/security-centre/844-20210304-core-xss-within-the-feed-parser-	A-JOO-JOOM-160321/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				library.html	
Improper Input Validation	04-Mar-21	5	An issue was discovered in Joomla! 3.2.0 through 3.9.24. Missing input validation within the template manager. **CVE ID : CVE-2021-23131**	https://developer.joomla.org/security-centre/845-20210305-core-input-validation-within-the-template-manager.html	A-JOO-JOOM-160321/150
Not Available	04-Mar-21	5	An issue was discovered in Joomla! 3.0.0 through 3.9.24. com_media allowed paths that are not intended for image uploads **CVE ID : CVE-2021-23132**	https://developer.joomla.org/security-centre/846-20210306-core-com-media-allowed-paths-that-are-not-intended-for-image-uploads.html	A-JOO-JOOM-160321/151
Exposure of Resource to Wrong Sphere	04-Mar-21	5	An issue was discovered in Joomla! 3.0.0 through 3.9.24. Incorrect ACL checks could allow unauthorized change of the category for an article. **CVE ID : CVE-2021-26027**	https://developer.joomla.org/security-centre/847-20210307-core-acl-violation-within-com-content-frontend-editing.html	A-JOO-JOOM-160321/152
Improper Limitation of a Pathname to a Restricted Directory	04-Mar-21	4.3	An issue was discovered in Joomla! 3.0.0 through 3.9.24. Extracting an specifilcy crafted zip package could write files	https://developer.joomla.org/security-centre/848-20210308-	A-JOO-JOOM-160321/153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			outside of the intended path. **CVE ID : CVE-2021-26028**	core-path-traversal-within-joomla-archive-zip-class.html	
Improper Input Validation	04-Mar-21	5	An issue was discovered in Joomla! 1.6.0 through 3.9.24. Inadequate filtering of form contents could allow to overwrite the author field. **CVE ID : CVE-2021-26029**	https://developer.joomla.org/security-centre/849-20210309-core-inadequate-filtering-of-form-contents-could-allow-to-overwrite-the-author-field.html	A-JOO-JOOM-160321/154
jpeg					
jpeg_xl					
Out-of-bounds Write	02-Mar-21	7.5	JPEG XL (aka jpeg-xl) through 0.3.2 allows writable memory corruption. **CVE ID : CVE-2021-27804**	N/A	A-JPE-JPEG-160321/155
jpeg-xl					
Out-of-bounds Write	05-Mar-21	6.8	jpeg-xl v0.3.2 is affected by a heap buffer overflow in /lib/jxl/coeff_order.cc ReadPermutation. When decoding a malicous jxl file using djxl, an attacker can trigger arbitrary code execution or a denial of service. **CVE ID : CVE-2021-28026**	N/A	A-JPE-JPEG-160321/156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Linuxfoundation					
argo_continuous_delivery					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-21	3.5	The package github.com/argoproj/argo-cd/cmd before 1.7.13, from 1.8.0 and before 1.8.6 are vulnerable to Cross-site Scripting (XSS) the SSO provider connected to Argo CD would have to send back a malicious error message containing JavaScript to the user. **CVE ID : CVE-2021-23347**	https://github.com/argoproj/argo-cd/pull/5563, https://snyk.io/vuln/SNYK-GOLANG-GITHUBCOMARGOPROJARGOCDCMD-1078291	A-LIN-ARGO-160321/157
lumis					
lumis_experience_platform					
Improper Restriction of XML External Entity Reference	03-Mar-21	6.4	LumisXP (aka Lumis Experience Platform) before 10.0.0 allows unauthenticated blind XXE via an API request to PageControllerXml.jsp. One can send a request crafted with an XXE payload and achieve outcomes such as reading local server files or denial of service. **CVE ID : CVE-2021-27931**	N/A	A-LUM-LUMI-160321/158
madge_project					
madge					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	09-Mar-21	7.5	This affects the package madge before 4.0.1. It is possible to specify a custom Graphviz path via the graphVizPath option parameter which when the .image(), .svg() or .dot() functions are called, is	https://github.com/pahen/madge/commit/da5cbc9ab30372d687fa7c324b22af7ffa5c6332, https://snyk.i	A-MAD-MADG-160321/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			executed by the childprocess.exec function. **CVE ID : CVE-2021-23352**	o/vuln/SNYK-JS-MADGE-1082875	
markdown2_project					
markdown2					
Not Available	03-Mar-21	5	markdown2 >=1.0.1.18, fixed in 2.4.0, is affected by a regular expression denial of service vulnerability. If an attacker provides a malicious string, it can make markdown2 processing difficult or delayed for an extended period of time. **CVE ID : CVE-2021-26813**	N/A	A-MAR-MARK-160321/160
matrix-react-sdk_project					
matrix-react-sdk					
Insufficient Verification of Data Authenticity	02-Mar-21	4.3	matrix-react-sdk is an npm package which is a Matrix SDK for React Javascript. In matrix-react-sdk before version 3.15.0, the user content sandbox can be abused to trick users into opening unexpected documents. The content is opened with a `blob` origin that cannot access Matrix user data, so messages and secrets are not at risk. This has been fixed in version 3.15.0. **CVE ID : CVE-2021-21320**	https://github.com/matrix-org/matrix-react-sdk/commit/b386f0c73b95ecbb6ea7f8f79c6ff5171a8dedd1, https://github.com/matrix-org/matrix-react-sdk/pull/5657, https://github.com/matrix-org/matrix-react-sdk/security/	A-MAT-MATR-160321/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				advisories/GHSA-52mq-6jcv-j79x	
Microsoft					
high_efficiency_video_coding					
Not Available	11-Mar-21	6.8	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062. **CVE ID : CVE-2021-24089**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24089	A-MIC-HIGH-160321/162
Not Available	11-Mar-21	6.8	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062. **CVE ID : CVE-2021-24110**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24110	A-MIC-HIGH-160321/163
Not Available	11-Mar-21	6.8	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26902	A-MIC-HIGH-160321/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			27062. **CVE ID : CVE-2021-26902**		
Not Available	11-Mar-21	6.8	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062. **CVE ID : CVE-2021-27047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27047	A-MIC-HIGH-160321/165
Not Available	11-Mar-21	6.8	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062. **CVE ID : CVE-2021-27048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27048	A-MIC-HIGH-160321/166
Not Available	11-Mar-21	6.8	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062. **CVE ID : CVE-2021-27049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27049	A-MIC-HIGH-160321/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	11-Mar-21	6.8	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062. **CVE ID : CVE-2021-27050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27050	A-MIC-HIGH-160321/168
Not Available	11-Mar-21	6.8	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27061, CVE-2021-27062. **CVE ID : CVE-2021-27051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27051	A-MIC-HIGH-160321/169
Not Available	11-Mar-21	6.8	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27062. **CVE ID : CVE-2021-27061**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27061	A-MIC-HIGH-160321/170
Not Available	11-Mar-21	6.8	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is	https://portal.msrc.microsoft.com/en-	A-MIC-HIGH-160321/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061. **CVE ID : CVE-2021-27062**	US/security-guidance/advisory/CVE-2021-27062	
exchange_server					
Not Available	03-Mar-21	6.5	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26854, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078. **CVE ID : CVE-2021-26412**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26412	A-MIC-EXCH-160321/172
Not Available	03-Mar-21	6.5	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26412, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078. **CVE ID : CVE-2021-26854**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26854	A-MIC-EXCH-160321/173
Not Available	03-Mar-21	7.5	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26412, CVE-2021-26854, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078. **CVE ID : CVE-2021-26855**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855	A-MIC-EXCH-160321/174
Not Available	03-Mar-21	6.8	Microsoft Exchange Server	https://porta	A-MIC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26412, CVE-2021-26854, CVE-2021-26855, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078. **CVE ID : CVE-2021-26857**	l.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26857	EXCH-160321/175
Not Available	03-Mar-21	6.8	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26412, CVE-2021-26854, CVE-2021-26855, CVE-2021-26857, CVE-2021-27065, CVE-2021-27078. **CVE ID : CVE-2021-26858**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26858	A-MIC-EXCH-160321/176
Not Available	03-Mar-21	6.8	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26412, CVE-2021-26854, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27078. **CVE ID : CVE-2021-27065**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27065	A-MIC-EXCH-160321/177
Not Available	03-Mar-21	6.5	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26412, CVE-2021-26854, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065. **CVE ID : CVE-2021-27078**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27078	A-MIC-EXCH-160321/178
minio					
minio					
Improper	08-Mar-21	4	MinIO is an open-source	https://githu	A-MIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			high performance object storage service and it is API compatible with Amazon S3 cloud storage service. In MinIO before version RELEASE.2021-03-04T00-53-13Z it is possible to bypass a readOnly policy by creating a temporary 'mc share upload' URL. Everyone is impacted who uses MinIO multi-users. This is fixed in version RELEASE.2021-03-04T00-53-13Z. As a workaround, one can disable uploads with `Content-Type: multipart/form-data` as mentioned in the S3 API RESTObjectPOST docs by using a proxy in front of MinIO. **CVE ID : CVE-2021-21362**	b.com/minio/minio/commit/039f59b552319fcc2f83631bb421a7d4b82bc482, https://github.com/minio/minio/security/advisories/GHSA-hq5j-6r98-9m8v	MINI-160321/179
Misp					
misp					
Not Available	02-Mar-21	2.1	An issue was discovered in app/Model/SharingGroupServer.php in MISP 2.4.139. In the implementation of Sharing Groups, the "all org" flag sometimes provided view access to unintended actors. **CVE ID : CVE-2021-27904**	https://github.com/MISP/MISP/commit/ca13fee271ad126832c88896776f3050a6c06e64	A-MIS-MISP-160321/180
Mozilla					
pollbot					
URL Redirection to	08-Mar-21	5.8	Pollbot is open source software which "frees its	https://github.com/mozill	A-MOZ-POLL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Untrusted Site ('Open Redirect')			human masters from the toilsome task of polling for the state of things during the Firefox release process." In Pollbot before version 1.4.4 there is an open redirection vulnerability in the path of "https://pollbot.services.mozilla.com/". An attacker can redirect anyone to malicious sites. To Reproduce type in this URL: "https://pollbot.services.mozilla.com//evil.com/". Affected versions will redirect to that website when you inject a payload like "//evil.com/". This is fixed in version 1.4.4. **CVE ID : CVE-2021-21354**	a/PollBot/commit/6db74a4fcbff258c7cdf51a6ff0724fc10c485e5, https://github.com/mozilla/PollBot/pull/333, https://github.com/mozilla/PollBot/security/advisories/GHSA-jhgx-wmq8-jc24	160321/181
nano_arena_project					
nano_arena					
Not Available	05-Mar-21	7.5	An issue was discovered in the nano_arena crate before 0.5.2 for Rust. There is an aliasing violation in split_at because two mutable references can exist for the same element, if Borrow<Idx> behaves in certain ways. This can have a resultant out-of-bounds write or use-after-free. **CVE ID : CVE-2021-28032**	https://rustsec.org/advisories/RUSTSEC-2021-0031.html	A-NAN-NANO-160321/182
newlib_project					
newlib					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Mar-21	7.5	A flaw was found in newlib in versions prior to 4.0.0. Improper overflow validation in the memory allocation functions mEMALIGn, pvALLOc, nano_memalign, nano_valloc, nano_pvalloc could case an integer overflow, leading to an allocation of a small buffer and then to a heap-based buffer overflow. **CVE ID : CVE-2021-3420**	https://bugzilla.redhat.com/show_bug.cgi?id=1934088	A-NEW-NEWL-160321/183
Nextcloud					
nextcloud_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-21	3.5	Nextcloud Server prior to 20.0.6 is vulnerable to reflected cross-site scripting (XSS) due to lack of sanitization in `OC.Notification.show`. **CVE ID : CVE-2021-22878**	https://github.com/nextcloud/server/pull/25234, https://nextcloud.com/security/advisory/?id=NC-SA-2021-005	A-NEX-NEXT-160321/184
nextcloud					
Improper Privilege Management	03-Mar-21	5.5	A missing user check in Nextcloud prior to 20.0.6 inadvertently populates a user's own credentials for other users external storage configuration when not already configured yet. **CVE ID : CVE-2021-22877**	https://github.com/nextcloud/server/issues/24600, https://github.com/nextcloud/server/pull/25224, https://nextcloud.com/security/advisory/?id=NC-SA-2021-004	A-NEX-NEXT-160321/185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Nodejs					
node.js					
Uncontrolled Resource Consumption	03-Mar-21	7.8	Node.js before 10.24.0, 12.21.0, 14.16.0, and 15.10.0 is vulnerable to a denial of service attack when too many connection attempts with an 'unknownProtocol' are established. This leads to a leak of file descriptors. If a file descriptor limit is configured on the system, then the server is unable to accept new connections and prevent the process also from opening, e.g. a file. If no file descriptor limit is configured, then this lead to an excessive memory usage and cause the system to run out of memory. **CVE ID : CVE-2021-22883**	https://nodejs.org/en/blog/vulnerability/february-2021-security-releases/	A-NOD-NODE-160321/186
Not Available	03-Mar-21	6.8	Node.js before 10.24.0, 12.21.0, 14.16.0, and 15.10.0 is vulnerable to DNS rebinding attacks as the whitelist includes “localhost6”. When “localhost6” is not present in /etc/hosts, it is just an ordinary domain that is resolved via DNS, i.e., over network. If the attacker controls the victim's DNS server or can spoof its responses, the DNS rebinding protection can be bypassed by using the	https://nodejs.org/en/blog/vulnerability/february-2021-security-releases/, https://nodejs.org/en/blog/vulnerability/march-2018-security-releases/#node-js-inspector-	A-NOD-NODE-160321/187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"localhost6" domain. As long as the attacker uses the "localhost6" domain, they can still apply the attack described in CVE-2018-7160. **CVE ID : CVE-2021-22884**	dns-rebinding-vulnerability-cve-2018-7160	
obss					
time_in_status					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Mar-21	3.5	In the "Time in Status" app before 4.13.0 for Jira, remote authenticated attackers can cause Stored XSS. **CVE ID : CVE-2021-27222**	https://dev.obss.com.tr/confluence/display/MD/2021-02-25+Time+in+Status+for+Jira+Server+and+Data+Center+Security+Advisory	A-OBS-TIME-160321/188
onlyoffice					
document_server					
Not Available	01-Mar-21	7.8	An improper binary stream data handling issue was found in the [core] module of ONLYOFFICE DocumentServer v4.0.0-9-v5.6.3. Using this bug, an attacker is able to produce a denial of service attack that can eventually shut down the target server. **CVE ID : CVE-2021-25829**	https://github.com/ONLYOFFICE/core, https://github.com/ONLYOFFICE/core/blob/c1e4a2ce33bdcfab29d670f5fdb10fc63cf5fd6a/ASCOfficePPTXFile/PPTXFormat/Comments.h#L299	A-ONL-DOCU-160321/189
Not Available	01-Mar-21	6.8	A file extension handling issue was found in [core]	N/A	A-ONL-DOCU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			module of ONLYOFFICE DocumentServer v4.2.0.236-v5.6.4.13. An attacker must request the conversion of the crafted file from DOCT into DOCX format. Using the chain of two other bugs related to improper string handling, an attacker can achieve remote code execution on DocumentServer. **CVE ID : CVE-2021-25830**		160321/190
Not Available	01-Mar-21	6.8	A file extension handling issue was found in [core] module of ONLYOFFICE DocumentServer v4.0.0-9-v5.6.3. An attacker must request the conversion of the crafted file from PPTT into PPTX format. Using the chain of two other bugs related to improper string handling, a remote attacker can obtain remote code execution on DocumentServer. **CVE ID : CVE-2021-25831**	https://github.com/merrychap/poc_exploits/tree/master/ONLYOFFICE/CVE-2021-25831, https://github.com/ONLYOFFICE/core, https://github.com/ONLYOFFICE/core/blob/v5.6.4.13/ASCOfficePPTXFile/Editor/BinaryFileReaderWriter.cpp#L1918	A-ONL-DOCU-160321/191
Out-of-bounds Write	01-Mar-21	6.8	A heap buffer overflow vulnerability inside of BMP image processing was found at [core] module of ONLYOFFICE DocumentServer v4.0.0-9-v6.0.0. Using this vulnerability, an attacker is	https://github.com/ONLYOFFICE/core, https://github.com/ONLYOFFICE/core/blob/v6.0.1.15/ASCOffice	A-ONL-DOCU-160321/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			able to gain remote code executions on DocumentServer. **CVE ID : CVE-2021-25832**	PPTXFile/Editor/BinaryFileReaderWriter.cpp#L424, https://github.com/ONLYOFFICE/core/blob/v6.0.1.15/ASCOfficePPTXFile/Editor/BinaryFileReaderWriter.cpp#L428	
Not Available	01-Mar-21	6.8	A file extension handling issue was found in [server] module of ONLYOFFICE DocumentServer v4.2.0.71-v5.6.0.21. The file extension is controlled by an attacker through the request data and leads to arbitrary file overwriting. Using this vulnerability, a remote attacker can obtain remote code execution on DocumentServer. **CVE ID : CVE-2021-25833**	https://github.com/ONLYOFFICE/DocumentServer	A-ONL-DOCU-160321/193
openark					
orchestrator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-21	4.3	resources/public/js/orchestrator.js in openark orchestrator before 3.2.4 allows XSS via the orchestrator-msg parameter. **CVE ID : CVE-2021-27940**	https://github.com/openark/orchestrator/pull/1313	A-OPE-ORCH-160321/194
Openbsd					
openssh					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	05-Mar-21	7.5	ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host. **CVE ID : CVE-2021-28041**	https://github.com/openssh/openssh-portable/commit/e04fd6dde16de1cdc5a4d9946397ff60d96568db, https://www.openssh.com/security.html, https://www.openssh.com/txt/release-8.5, https://www.openwall.com/lists/oss-security/2021/03/03/1	A-OPE-OPEN-160321/195
Opensuse					
tumbleweed					
Incorrect Implementation of Authentication Algorithm	03-Mar-21	4.6	A Incorrect Implementation of Authentication Algorithm vulnerability in of SUSE SUSE Linux Enterprise Server 15 SP 3; openSUSE Tumbleweed allows local attackers to execute arbitrary code via salt without the need to specify valid credentials. This issue affects: SUSE SUSE Linux Enterprise Server 15 SP 3 salt versions prior to 3002.2-3. openSUSE Tumbleweed salt version	https://bugzilla.suse.com/show_bug.cgi?id=1182382	A-OPE-TUMB-160321/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3002.2-2.1 and prior versions. **CVE ID : CVE-2021-25315**		
Oracle					
cloud_infrastructure_data_science					
Not Available	03-Mar-21	4.1	Vulnerability in the Oracle Cloud Infrastructure Data Science Notebook Sessions. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the Oracle Cloud Infrastructure Data Science Notebook Sessions executes to compromise Oracle Cloud Infrastructure Data Science Notebook Sessions. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Cloud Infrastructure Data Science Notebook Sessions accessible data as well as unauthorized read access to a subset of Oracle Cloud Infrastructure Data Science Notebook Sessions accessible data. All affected customers were notified of CVE-2021-2138 by Oracle. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L	N/A	A-ORA-CLOU-160321/197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/UI:N/S:U/C:L/I:L/A:N) **CVE ID : CVE-2021-2138**		
oryx-embedded					
cyclonetcp					
Improper Input Validation	08-Mar-21	5	Oryx Embedded CycloneTCP 1.7.6 to 2.0.0, fixed in 2.0.2, is affected by incorrect input validation, which may cause a denial of service (DoS). To exploit the vulnerability, an attacker needs to have TCP connectivity to the target system. Receiving a maliciously crafted TCP packet from an unauthenticated endpoint is sufficient to trigger the bug. **CVE ID : CVE-2021-26788**	https://github.com/Oryx-Embedded/CycloneTCP/commit/de5336016edbe1e90327d0ed1cba5c4e4911436 6?branch=de5336016edbe1e90327d0ed1cba5c4e491 14366&diff=split	A-ORY-CYCL-160321/198
Ossec					
ossec					
Uncontrolled Recursion	05-Mar-21	5	An issue was discovered in OSSEC 3.6.0. An uncontrolled recursion vulnerability in os_xml.c occurs when a large number of opening and closing XML tags is used. Because recursion is used in _ReadElem without restriction, an attacker can trigger a segmentation fault once unmapped memory is reached. **CVE ID : CVE-2021-28040**	N/A	A-OSS-OSSE-160321/199
ougc_feedback_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ougc_feedback					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-21	4.3	The OUGC Feedback plugin before 1.8.23 for MyBB allows XSS via the comment field of feedback during an edit operation. **CVE ID : CVE-2021-28115**	https://github.com/Sama34/OUGC-Feedback/pull/31/commits/ceef7c06359e5dcbaffe90a40884265c5754068c	A-OUG-OUGC-160321/200
Privoxy					
privoxy					
Reachable Assertion	09-Mar-21	5	A flaw was found in privoxy before 3.0.32. An assertion failure could be triggered with a crafted CGI request leading to server crash. **CVE ID : CVE-2021-20272**	https://bugzilla.redhat.com/show_bug.cgi?id=1936651, https://www.privoxy.org/announce.txt	A-PRI-PRIV-160321/201
Improper Input Validation	09-Mar-21	5	A flaw was found in privoxy before 3.0.32. A crash can occur via a crafted CGI request if Privoxy is toggled off. **CVE ID : CVE-2021-20273**	https://bugzilla.redhat.com/show_bug.cgi?id=1936658, https://www.privoxy.org/announce.txt	A-PRI-PRIV-160321/202
NULL Pointer Dereference	09-Mar-21	5	A flaw was found in privoxy before 3.0.32. A crash may occur due a NULL-pointer dereference when the socks server misbehaves. **CVE ID : CVE-2021-20274**	https://bugzilla.redhat.com/show_bug.cgi?id=1936662, https://www.privoxy.org/announce.txt	A-PRI-PRIV-160321/203
Improper Restriction of Operations	09-Mar-21	5	A flaw was found in privoxy before 3.0.32. A invalid read of size two	https://bugzilla.redhat.com/show_bug.	A-PRI-PRIV-160321/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			may occur in chunked_body_is_complete() leading to denial of service. **CVE ID : CVE-2021-20275**	cgi?id=1936666, https://www.privoxy.org/announce.txt	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-21	5	A flaw was found in privoxy before 3.0.32. Invalid memory access with an invalid pattern passed to pcre_compile() may lead to denial of service. **CVE ID : CVE-2021-20276**	https://bugzilla.redhat.com/show_bug.cgi?id=1936668, https://www.privoxy.org/announce.txt	A-PRI-PRIV-160321/205
pugjs					
pug					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Mar-21	6.8	Pug is an npm package which is a high-performance template engine. In pug before version 3.0.1, if a remote attacker was able to control the `pretty` option of the pug compiler, e.g. if you spread a user provided object such as the query parameters of a request into the pug template inputs, it was possible for them to achieve remote code execution on the node.js backend. This is fixed in version 3.0.1. This advisory applies to multiple pug packages including "pug", "pug-code-gen". pug-code-gen has a backported fix at version 2.0.3. This advisory is not exploitable if there is no	https://github.com/pugjs/pug/commit/991e78f7c4220b2f8da042877c6f0ef5a4683be0, https://github.com/pugjs/pug/issues/3312, https://github.com/pugjs/pug/pull/3314, https://github.com/pugjs/pug/security/advisories/GHSA-p493-635q-r6gr	A-PUG-PUG-160321/206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			way for un-trusted input to be passed to pug as the `pretty` option, e.g. if you compile templates in advance before applying user input to them, you do not need to upgrade. **CVE ID : CVE-2021-21353**		
pug-code-gen					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Mar-21	6.8	Pug is an npm package which is a high-performance template engine. In pug before version 3.0.1, if a remote attacker was able to control the `pretty` option of the pug compiler, e.g. if you spread a user provided object such as the query parameters of a request into the pug template inputs, it was possible for them to achieve remote code execution on the node.js backend. This is fixed in version 3.0.1. This advisory applies to multiple pug packages including "pug", "pug-code-gen". pug-code-gen has a backported fix at version 2.0.3. This advisory is not exploitable if there is no way for un-trusted input to be passed to pug as the `pretty` option, e.g. if you compile templates in advance before applying user input to them, you do not need to upgrade.	https://github.com/pugjs/pug/commit/991e78f7c4220b2f8da042877c6f0ef5a4683be0, https://github.com/pugjs/pug/issues/3312, https://github.com/pugjs/pug/pull/3314, https://github.com/pugjs/pug/security/advisories/GHSA-p493-635q-r6gr	A-PUG-PUG-160321/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21353		
Python					
pillow					
Uncontrolled Resource Consumption	03-Mar-21	5	Pillow before 8.1.1 allows attackers to cause a denial of service (memory consumption) because the reported size of a contained image is not properly checked for a BLP container, and thus an attempted memory allocation can be very large. **CVE ID : CVE-2021-27921**	https://pillow.readthedocs.io/en/stable/releasenotes/8.1.1.html	A-PYT-PILL-160321/208
Uncontrolled Resource Consumption	03-Mar-21	5	Pillow before 8.1.1 allows attackers to cause a denial of service (memory consumption) because the reported size of a contained image is not properly checked for an ICNS container, and thus an attempted memory allocation can be very large. **CVE ID : CVE-2021-27922**	https://pillow.readthedocs.io/en/stable/releasenotes/8.1.1.html	A-PYT-PILL-160321/209
Uncontrolled Resource Consumption	03-Mar-21	5	Pillow before 8.1.1 allows attackers to cause a denial of service (memory consumption) because the reported size of a contained image is not properly checked for an ICO container, and thus an attempted memory allocation can be very large.	https://pillow.readthedocs.io/en/stable/releasenotes/8.1.1.html	A-PYT-PILL-160321/210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-27923		
quinn_project					
quinn					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Mar-21	5	An issue was discovered in the quinn crate before 0.7.0 for Rust. It may have invalid memory access for certain versions of the standard library because it relies on a direct cast of std::net::SocketAddrV4 and std::net::SocketAddrV6 data structures. **CVE ID : CVE-2021-28036**	https://rustsec.org/advisories/RUSTSEC-2021-0035.html	A-QUI-QUIN-160321/211
rancher					
rancher					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Mar-21	4.3	A Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rancher allows remote attackers to execute JavaScript via malicious links. This issue affects: SUSE Rancher Rancher versions prior to 2.5.6. **CVE ID : CVE-2021-25313**	https://bugzilla.suse.com/show_bug.cgi?id=1181852, https://github.com/rancher/rancher/issues/31583, https://github.com/rancher/rancher/releases/tag/v2.5.6	A-RAN-RANC-160321/212
ratcf					
ratcf					
Improper Authentication	08-Mar-21	6.8	RATCF is an open-source framework for hosting Cyber-Security Capture the Flag events. In affected versions of RATCF users with multi factor authentication enabled are	https://github.com/ractf/core/commit/c57a4d186bfc586ad3edfe4dcba9f11efbf22f09#diff-	A-RAT-RATC-160321/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			able to log in without a valid token. This is fixed in commit cebb67b. **CVE ID : CVE-2021-21329**	60c444c47c061306f2dff5bf97c07810f40f949a8e94ecbb609b6b29364c8642R130-R152, https://github.com/ractf/core/commit/cebb67bd16a829612120180533236 5ffccb29638	
Redhat					
openshift_container_platform					
Improper Control of Generation of Code ('Code Injection')	09-Mar-21	4.6	A flaw was found in the Linux kernel in versions prior to 5.10. A violation of memory access was found while detecting a padding of int3 in the linking state. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3411**	http://blog.pi3.com.pl/?p=831	A-RED-OPEN-160321/214
Rockwellautomation					
studio_5000_logix_designer					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769,	N/A	A-ROC-STUD-160321/215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
rslogix_500					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix	N/A	A-ROC-RSLO-160321/216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
Saltstack					
salt					
Incorrect Implementation of Authentication Algorithm	03-Mar-21	4.6	A Incorrect Implementation of Authentication Algorithm vulnerability in of SUSE SUSE Linux Enterprise Server 15 SP 3; openSUSE Tumbleweed allows local attackers to execute arbitrary code via salt without the need to specify valid credentials. This issue affects: SUSE SUSE Linux Enterprise Server 15 SP 3 salt versions prior to	https://bugzilla.suse.com/show_bug.cgi?id=1182382	A-SAL-SALT-160321/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3002.2-3. openSUSE Tumbleweed salt version 3002.2-2.1 and prior versions. **CVE ID : CVE-2021-25315**		
Samsung					
pay_mini					
Exposure of Sensitive Information to an Unauthorized Actor	04-Mar-21	1.9	Improper access control in Samsung Pay mini application prior to v4.0.14 allows unauthorized access to balance information over the lockscreen in specific condition. **CVE ID : CVE-2021-25331**	https://security.samsungmobile.com, https://security.samsungmobile.com/serviceWeb.smsb	A-SAM-PAY_-160321/218
Exposure of Sensitive Information to an Unauthorized Actor	04-Mar-21	1.9	Improper access control in Samsung Pay mini application prior to v4.0.14 allows unauthorized access to contacts information over the lockscreen in specific condition. **CVE ID : CVE-2021-25332**	https://security.samsungmobile.com, https://security.samsungmobile.com/serviceWeb.smsb	A-SAM-PAY_-160321/219
Exposure of Sensitive Information to an Unauthorized Actor	04-Mar-21	1.9	Improper access control in Samsung Pay mini application prior to v4.0.14 allows unauthorized access to balance information over the lockscreen via scanning specific QR code. **CVE ID : CVE-2021-25333**	https://security.samsungmobile.com, https://security.samsungmobile.com/serviceWeb.smsb	A-SAM-PAY_-160321/220
one_ui					
Not Available	04-Mar-21	1.9	Improper lockscreen status check in cocktailbar service in Samsung mobile devices prior to SMR Mar-2021 Release 1 allows unauthenticated users to	https://security.samsungmobile.com, https://security.samsungmobile.com/sec	A-SAM-ONE_-160321/221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access hidden notification contents over the lockscreen in specific condition. **CVE ID : CVE-2021-25335**	urityUpdate.smsb	
s_assistant					
Improper Authentication	04-Mar-21	2.1	Calling of non-existent provider in S Assistant prior to version 6.5.01.22 allows unauthorized actions including denial of service attack by hijacking the provider. **CVE ID : CVE-2021-25341**	https://security.samsungmobile.com, https://security.samsungmobile.com/serviceWeb.smsb	A-SAM-S_AS-160321/222
members					
Improper Authentication	04-Mar-21	2.1	Calling of non-existent provider in SMP sdk prior to version 3.0.9 allows unauthorized actions including denial of service attack by hijacking the provider. **CVE ID : CVE-2021-25342**	https://security.samsungmobile.com, https://security.samsungmobile.com/serviceWeb.smsb	A-SAM-MEMB-160321/223
Improper Authentication	04-Mar-21	2.1	Calling of non-existent provider in Samsung Members prior to version 2.4.81.13 (in Android O(8.1) and below) and 3.8.00.13 (in Android P(9.0) and above) allows unauthorized actions including denial of service attack by hijacking the provider. **CVE ID : CVE-2021-25343**	https://security.samsungmobile.com/, https://security.samsungmobile.com/serviceWeb.smsb	A-SAM-MEMB-160321/224
internet					
Not Available	04-Mar-21	2.1	Improper permission grant check in Samsung Internet	https://security.samsungm	A-SAM-INTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to version 13.0.1.60 allows access to files in internal storage without authorized STORAGE permission. **CVE ID : CVE-2021-25348**	obile.com/, https://security.samsungmobile.com/serviceWeb.smsb	160321/225
SAP					
3d_visual_enterprise_viewer					
Not Available	09-Mar-21	4.3	When a user opens manipulated PhotoShop Document (.PSD) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2021-27584**	https://launchpad.support.sap.com/#/notes/3027758, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=571343107	A-SAP-3D_V-160321/226
Not Available	09-Mar-21	4.3	When a user opens manipulated Computer Graphics Metafile (.CGM) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2021-27585**	https://launchpad.support.sap.com/#/notes/3027758, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=571343107	A-SAP-3D_V-160321/227
Not Available	09-Mar-21	4.3	When a user opens manipulated Interchange File Format (.IFF) format files received from	https://launchpad.support.sap.com/#/notes/302775	A-SAP-3D_V-160321/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2021-27586**	8, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=571343107	
Not Available	09-Mar-21	4.3	When a user opens manipulated Jupiter Tessellation (.JT) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2021-27587**	https://launchpad.support.sap.com/#/notes/3027758, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=571343107	A-SAP-3D_V-160321/229
Not Available	09-Mar-21	4.3	When a user opens manipulated HPGL format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2021-27588**	https://launchpad.support.sap.com/#/notes/3027758, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=571343107	A-SAP-3D_V-160321/230
Not Available	09-Mar-21	4.3	When a user opens manipulated Scalable Vector Graphics (.SVG) format files received from untrusted sources in SAP	https://launchpad.support.sap.com/#/notes/3027758,	A-SAP-3D_V-160321/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2021-27589**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=571343107	
Not Available	09-Mar-21	4.3	When a user opens manipulated Tag Image File Format (.TIFF) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2021-27590**	https://launchpad.support.sap.com/#/notes/3027758, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=571343107	A-SAP-3D_V-160321/232
Not Available	09-Mar-21	4.3	When a user opens manipulated Portable Document Format (.PDF) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2021-27591**	https://launchpad.support.sap.com/#/notes/3027758, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=571343107	A-SAP-3D_V-160321/233
Not Available	09-Mar-21	4.3	When a user opens manipulated Universal 3D (.U3D) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application	https://launchpad.support.sap.com/#/notes/3027767, https://wiki.s	A-SAP-3D_V-160321/234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crashes and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2021-27592**	cn.sap.com/wiki/pages/viewpage.action?pageId=571343107	
scratchpad_project					
scratchpad					
Double Free	05-Mar-21	7.5	An issue was discovered in the scratchpad crate before 1.3.1 for Rust. The move_elements function can have a double-free upon a panic in a user-provided f function. **CVE ID : CVE-2021-28031**	https://rustsec.org/advisories/RUSTSEC-2021-0030.html	A-SCR-SCRA-160321/235
sfcyazilim					
sonlogger					
Incorrect Permission Assignment for Critical Resource	05-Mar-21	6.4	SonLogger before 6.4.1 is affected by user creation with any user permissions profile (e.g., SuperAdmin). An anonymous user can send a POST request to /User/saveUser without any authentication or session header. **CVE ID : CVE-2021-27963**	https://www.sonlogger.com/releasenotes	A-SFC-SONL-160321/236
Unrestricted Upload of File with Dangerous Type	05-Mar-21	7.5	SonLogger before 6.4.1 is affected by Unauthenticated Arbitrary File Upload. An attacker can send a POST request to /Config/SaveUploadedHotspotLogoFile without any authentication or session header. There is no check for the file extension or content of the uploaded	https://www.sonlogger.com/releasenotes	A-SFC-SONL-160321/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file. **CVE ID : CVE-2021-27964**		
spnego_http_authentication_module_project					
spnego_http_authentication_module					
Improper Authentication	08-Mar-21	7.5	In the SPNEGO HTTP Authentication Module for nginx (spnego-http-auth-nginx-module) before version 1.1.1 basic Authentication can be bypassed using a malformed username. This affects users of spnego-http-auth-nginx-module that have enabled basic authentication. This is fixed in version 1.1.1 of spnego-http-auth-nginx-module. As a workaround, one may disable basic authentication. **CVE ID : CVE-2021-21335**	https://github.com/stnoonan/spnego-http-auth-nginx-module/commit/a06f9efca373e25328b1c53639a48decd0854570, https://github.com/stnoonan/spnego-http-auth-nginx-module/security/advisories/GHSA-ww8q-72rx-hc54	A-SPN-SPNE-160321/238
squarebox					
catdv					
Missing Authentication for Critical Function	05-Mar-21	6.4	An issue was discovered in SquareBox CatDV Server through 9.2. An attacker can invoke sensitive RMI methods such as getConnections without authentication, the results of which can be used to generate valid authentication tokens. These tokens can then be used to invoke administrative tasks within	N/A	A-SQU-CATD-160321/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the application, such as disclosing password hashes. **CVE ID : CVE-2021-26705**		
Squid-cache					
squid					
Out-of-bounds Read	09-Mar-21	4.3	Squid through 4.14 and 5.x through 5.0.5, in some configurations, allows information disclosure because of an out-of-bounds read in WCCP protocol data. This can be leveraged as part of a chain for remote code execution as nobody. **CVE ID : CVE-2021-28116**	http://www.squid-cache.org/Versions/	A-SQU-SQUI-160321/240
stack_dst_project					
stack_dst					
Double Free	05-Mar-21	7.5	An issue was discovered in the stack_dst crate before 0.6.1 for Rust. Because of the push_inner behavior, a double free can occur upon a val.clone() panic. **CVE ID : CVE-2021-28034**	https://rustsec.org/advisories/RUSTSEC-2021-0033.html	A-STA-STAC-160321/241
Not Available	05-Mar-21	7.5	An issue was discovered in the stack_dst crate before 0.6.1 for Rust. Because of the push_inner behavior, a drop of uninitialized memory can occur upon a val.clone() panic. **CVE ID : CVE-2021-28035**	https://rustsec.org/advisories/RUSTSEC-2021-0033.html	A-STA-STAC-160321/242
stormshield					
network_security					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	02-Mar-21	5	A vulnerability in Stormshield Network Security could allow an attacker to trigger a protection related to ARP/NDP tables management, which would temporarily prevent the system to contact new hosts via IPv4 or IPv6. This affects versions 2.0.0 to 2.7.7, 2.8.0 to 2.16.0, 3.0.0 to 3.7.16, 3.8.0 to 3.11.4, and 4.0.0 to 4.1.5. Fixed in versions 2.7.8, 3.7.17, 3.11.5, and 4.2.0. **CVE ID : CVE-2021-3384**	https://advisories.stormshield.eu/2020-049/	A-STO-NETW-160321/243
Tenable					
tenable.sc					
Deserialization of Untrusted Data	03-Mar-21	6.5	Tenable.sc and Tenable.sc Core versions 5.13.0 through 5.17.0 were found to contain a vulnerability that could allow an authenticated, unprivileged user to perform Remote Code Execution (RCE) on the Tenable.sc server via Hypertext Preprocessor unserialization. **CVE ID : CVE-2021-20076**	https://www.tenable.com/security/tns-2021-03	A-TEN-TENA-160321/244
toodee_project					
toodee					
Double Free	05-Mar-21	7.5	An issue was discovered in the toodee crate before 0.3.0 for Rust. Row insertion can cause a double free upon an	https://rustsec.org/advisories/RUSTSEC-2021-0028.html	A-TOO-TOOD-160321/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iterator panic. **CVE ID : CVE-2021-28028**		
Not Available	05-Mar-21	5	An issue was discovered in the toodee crate before 0.3.0 for Rust. The row-insertion feature allows attackers to read the contents of uninitialized memory locations. **CVE ID : CVE-2021-28029**	https://rustsec.org/advisories/RUSTSEC-2021-0028.html	A-TOO-TOOD-160321/246
totaljs					
total.js					
Improper Control of Generation of Code ('Code Injection')	04-Mar-21	7.5	The package total.js before 3.4.8 are vulnerable to Remote Code Execution (RCE) via set. **CVE ID : CVE-2021-23344**	https://github.com/totaljs/framework/commit/c812bbcab8981797d3a1b9993fc42dad3d246f04, https://snyk.io/vuln/SNYK-JS-TOTALJS-1077069	A-TOT-TOTA-160321/247
truetype_project					
truetype					
Use of Uninitialized Resource	05-Mar-21	5	An issue was discovered in the truetype crate before 0.30.1 for Rust. Attackers can read the contents of uninitialized memory locations via a user-provided Read operation within Tape::take_bytes. **CVE ID : CVE-2021-28030**	https://rustsec.org/advisories/RUSTSEC-2021-0029.html	A-TRU-TRUE-160321/248
Veritas					
backup_exec					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	01-Mar-21	7.5	An issue was discovered in Veritas Backup Exec before 21.2. The communication between a client and an Agent requires successful authentication, which is typically completed over a secure TLS communication. However, due to a vulnerability in the SHA Authentication scheme, an attacker is able to gain unauthorized access and complete the authentication process. Subsequently, the client can execute data management protocol commands on the authenticated connection. By using crafted input parameters in one of these commands, an attacker can access an arbitrary file on the system using System privileges. **CVE ID : CVE-2021-27876**	https://www.veritas.com/content/support/en_US/security/VTS21-001#issue2	A-VER-BACK-160321/249
Improper Authentication	01-Mar-21	7.5	An issue was discovered in Veritas Backup Exec before 21.2. It supports multiple authentication schemes: SHA authentication is one of these. This authentication scheme is no longer used in current versions of the product, but hadn't yet been disabled. An attacker could remotely exploit this scheme to gain unauthorized access to an	https://www.veritas.com/content/support/en_US/security/VTS21-001#issue1	A-VER-BACK-160321/250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Agent and execute privileged commands. **CVE ID : CVE-2021-27877**		
Improper Authentication	01-Mar-21	9	An issue was discovered in Veritas Backup Exec before 21.2. The communication between a client and an Agent requires successful authentication, which is typically completed over a secure TLS communication. However, due to a vulnerability in the SHA Authentication scheme, an attacker is able to gain unauthorized access and complete the authentication process. Subsequently, the client can execute data management protocol commands on the authenticated connection. The attacker could use one of these commands to execute an arbitrary command on the system using system privileges. **CVE ID : CVE-2021-27878**	https://www.veritas.com/content/support/en_US/security/VTS21-001#issue3	A-VER-BACK-160321/251
Vmware					
view_planner					
Unrestricted Upload of File with Dangerous Type	03-Mar-21	7.5	VMware View Planner 4.x prior to 4.6 Security Patch 1 contains a remote code execution vulnerability. Improper input validation and lack of authorization leading to arbitrary file upload in logupload web	https://www.vmware.com/security/advisories/VMSA-2021-0003.html	A-VMW-VIEW-160321/252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application. An unauthorized attacker with network access to View Planner Harness could upload and execute a specially crafted file leading to remote code execution within the logupload container. **CVE ID : CVE-2021-21978**		
spring_integration_zip					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-21	5	Addresses partial fix in CVE-2018-1263. Spring-integration-zip, versions prior to 1.0.4, exposes an arbitrary file write vulnerability, that can be achieved using a specially crafted zip archive (affects other archives as well, bzip2, tar, xz, war, cpio, 7z), that holds path traversal filenames. So when the filename gets concatenated to the target extraction directory, the final path ends up outside of the target folder. **CVE ID : CVE-2021-22114**	https://tanzu.vmware.com/security/cve-2021-22114	A-VMW-SPRI-160321/253
wazuh					
wazuh					
Improper Input Validation	06-Mar-21	6.5	Wazuh API in Wazuh from 4.0.0 to 4.0.3 allows authenticated users to execute arbitrary code with administrative privileges via /manager/files URI. An authenticated user to the service may exploit	https://documentation.wazuh.com/4.0/release-notes/release_4_0_4.html	A-WAZ-WAZU-160321/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			incomplete input validation on the /manager/files API to inject arbitrary code within the API service script. **CVE ID : CVE-2021-26814**		
web_based_quiz_system_project					
web_based_quiz_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-21	4.3	Web Based Quiz System 1.0 is affected by cross-site scripting (XSS) in admin.php through the options parameter. **CVE ID : CVE-2021-28006**	N/A	A-WEB-WEB_-160321/255
wpserveur					
wps_hide_login					
Incorrect Authorization	01-Mar-21	7.5	WPS Hide Login 1.6.1 allows remote attackers to bypass a protection mechanism via post_password. **CVE ID : CVE-2021-3332**	N/A	A-WPS-WPS_-160321/256
ymfe					
yapi					
Use of Insufficiently Random Values	01-Mar-21	3.6	Weak JSON Web Token (JWT) signing secret generation in YMFE YApi through 1.9.2 allows recreation of other users' JWT tokens. This occurs because Math.random in Node.js is used. **CVE ID : CVE-2021-27884**	N/A	A-YMF-YAPI-160321/257
ytnef_project					
ytnef					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	04-Mar-21	6.8	In ytnef 1.9.3, the TNEFSubjectHandler function in lib/ytnef.c allows remote attackers to cause a denial-of-service (and potentially code execution) due to a double free which can be triggered via a crafted file. **CVE ID : CVE-2021-3403**	N/A	A-YTN-YTNE-160321/258
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Mar-21	6.8	In ytnef 1.9.3, the SwapWord function in lib/ytnef.c allows remote attackers to cause a denial-of-service (and potentially code execution) due to a heap buffer overflow which can be triggered via a crafted file. **CVE ID : CVE-2021-3404**	N/A	A-YTN-YTNE-160321/259
yubico					
yubihsm-shell					
Out-of-bounds Read	04-Mar-21	4.3	An issue was discovered in the _send_secure_msg() function of Yubico yubihsm-shell through 2.0.3. The function does not correctly validate the embedded length field of an authenticated message received from the device. Out-of-bounds reads performed by aes_remove_padding() can crash the running process, depending on the memory layout. This could be used by an attacker to cause a client-side denial of service.	https://www.yubico.com/support/security-advisories/ysa-2021-01/	A-YUB-YUBI-160321/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The yubihsm-shell project is included in the YubiHSM 2 SDK product. **CVE ID : CVE-2021-27217**		
Zend					
Zendto					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-21	4.3	ZendTo before 6.06-4 Beta allows XSS during the display of a drop-off in which a filename has unexpected characters. **CVE ID : CVE-2021-27888**	https://zend.to/changelog.php	A-ZEN-ZEND-160321/261
Zope					
products.genericsetup					
Exposure of Sensitive Information to an Unauthorized Actor	09-Mar-21	5	Products.GenericSetup is a mini-framework for expressing the configured state of a Zope Site as a set of filesystem artifacts. In Products.GenericSetup before version 2.1.1 there is an information disclosure vulnerability - anonymous visitors may view log and snapshot files generated by the Generic Setup Tool. The problem has been fixed in version 2.1.1. Depending on how you have installed Products.GenericSetup, you should change the buildout version pin to 2.1.1 and re-run the buildout, or if you used pip simply do pip install `"Products.GenericSetup>=	https://github.com/zopefoundation/Products.GenericSetup/commit/700319512b3615b3871a1f24e096cf66dc488c57, https://github.com/zopefoundation/Products.GenericSetup/security/advisories/GHSA-jff3-mwp3-f8cw	A-ZOP-PROD-160321/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.1.1"`. **CVE ID : CVE-2021-21360**		
products.pluggableauthservice					
Exposure of Sensitive Information to an Unauthorized Actor	08-Mar-21	4	Products.PluggableAuthService is a pluggable Zope authentication and authorization framework. In Products.PluggableAuthService before version 2.6.0 there is an information disclosure vulnerability - everyone can list the names of roles defined in the ZODB Role Manager plugin if the site uses this plugin. The problem has been fixed in version 2.6.0. Depending on how you have installed Products.PluggableAuthService, you should change the buildout version pin to 2.6.0 and re-run the buildout, or if you used pip simply do `pip install "Products.PluggableAuthService>=2.6.0"`. **CVE ID : CVE-2021-21336**	https://github.com/zopefoundation/Products.PluggableAuthService/commit/2dad81128250cb2e5d950cddc9d3c0314a80b4bb, https://github.com/zopefoundation/Products.PluggableAuthService/security/advisories/GHSA-p75f-g7gx-2r7p	A-ZOP-PROD-160321/263
URL Redirection to Untrusted Site ('Open Redirect')	08-Mar-21	5.8	Products.PluggableAuthService is a pluggable Zope authentication and authorization framework. In Products.PluggableAuthService before version 2.6.0 there is an open redirect vulnerability. A maliciously crafted link to the login form and login	https://github.com/zopefoundation/Products.PluggableAuthService/commit/7eead067898852ebd3e0f143bc51295928528dfa, https://githu	A-ZOP-PROD-160321/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functionality could redirect the browser to a different website. The problem has been fixed in version 2.6.1. Depending on how you have installed Products.PluggableAuthService, you should change the buildout version pin to `2.6.1` and re-run the buildout, or if you used `pip` simply do `pip install "Products.PluggableAuthService>=2.6.1". **CVE ID : CVE-2021-21337**	b.com/zopefoundation/Products.PluggableAuthService/security/advisories/GHSA-p44j-xrqg-4xrr	
Operating System					
Apple					
iphone_os					
Origin Validation Error	09-Mar-21	4.3	Insufficient data validation in Reader Mode in Google Chrome on iOS prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page and a malicious server. **CVE ID : CVE-2021-21163**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	O-APP-IPHO-160321/265
Origin Validation Error	09-Mar-21	4.3	Insufficient data validation in Chrome on iOS in Google Chrome on iOS prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-21164**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	O-APP-IPHO-160321/266
Incorrect Authorization	09-Mar-21	4.3	Insufficient policy enforcement in QR scanning in Google Chrome	https://chromereleases.googleblog.co	O-APP-IPHO-160321/267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on iOS prior to 89.0.4389.72 allowed an attacker who convinced the user to scan a QR code to bypass navigation restrictions via a crafted QR code. **CVE ID : CVE-2021-21186**	m/2021/03/stable-channel-update-for-desktop.html	
Debian					
debian_linux					
Reachable Assertion	09-Mar-21	5	A flaw was found in privoxy before 3.0.32. An assertion failure could be triggered with a crafted CGI request leading to server crash. **CVE ID : CVE-2021-20272**	https://bugzilla.redhat.com/show_bug.cgi?id=1936651, https://www.privoxy.org/announce.txt	O-DEB-DEBI-160321/268
Improper Input Validation	09-Mar-21	5	A flaw was found in privoxy before 3.0.32. A crash can occur via a crafted CGI request if Privoxy is toggled off. **CVE ID : CVE-2021-20273**	https://bugzilla.redhat.com/show_bug.cgi?id=1936658, https://www.privoxy.org/announce.txt	O-DEB-DEBI-160321/269
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-21	5	A flaw was found in privoxy before 3.0.32. A invalid read of size two may occur in chunked_body_is_complete() leading to denial of service. **CVE ID : CVE-2021-20275**	https://bugzilla.redhat.com/show_bug.cgi?id=1936666, https://www.privoxy.org/announce.txt	O-DEB-DEBI-160321/270
Improper Restriction of Operations within the	09-Mar-21	5	A flaw was found in privoxy before 3.0.32. Invalid memory access with an invalid pattern	https://bugzilla.redhat.com/show_bug.cgi?id=19366	O-DEB-DEBI-160321/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			passed to pcre_compile() may lead to denial of service. **CVE ID : CVE-2021-20276**	68, https://www.privoxy.org/announce.txt	
Dell					
emc_powerscale_onefs					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Mar-21	4.6	PowerScale OneFS 8.1.2,8.2.2 and 9.1.0 contains an improper input sanitization issue in a command. The Compadmin user could potentially exploit this vulnerability, leading to potential privileges escalation. **CVE ID : CVE-2021-21503**	https://www.dell.com/support/kbdoc/000183717	O-DEL-EMC_-160321/272
Improper Input Validation	08-Mar-21	6.5	PowerScale OneFS 8.1.2,8.2.2 and 9.1.0 contains an improper input sanitization issue in its API handler. An un-authtenticated with ISI_PRIV_SYS_SUPPORT and ISI_PRIV_LOGIN_PAPI privileges could potentially exploit this vulnerability, leading to potential privileges escalation. **CVE ID : CVE-2021-21506**	https://www.dell.com/support/kbdoc/000183717	O-DEL-EMC_-160321/273
idrac8_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Mar-21	5.8	Dell iDRAC8 versions prior to 2.75.100.75 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary 'Host' header	https://www.dell.com/support/kbdoc/en-us/000183758/dsa-2021-041-dell-emc-idrac-8-	O-DEL-IDRA-160321/274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			values to poison a web-cache or trigger redirections. **CVE ID : CVE-2021-21510**	security-update-for-a-host-header-injection-vulnerability	
Fedoraproject					
fedora					
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-20225**	N/A	O-FED-FEDO-160321/275
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and	https://bugzilla.redhat.com/show_bug.cgi?id=1926263	O-FED-FEDO-160321/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			integrity as well as system availability. **CVE ID : CVE-2021-20233**		
Use After Free	04-Mar-21	6.8	In ytnef 1.9.3, the TNEFSubjectHandler function in lib/ytnef.c allows remote attackers to cause a denial-of-service (and potentially code execution) due to a double free which can be triggered via a crafted file. **CVE ID : CVE-2021-3403**	N/A	O-FED-FEDO-160321/277
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Mar-21	6.8	In ytnef 1.9.3, the SwapWord function in lib/ytnef.c allows remote attackers to cause a denial-of-service (and potentially code execution) due to a heap buffer overflow which can be triggered via a crafted file. **CVE ID : CVE-2021-3404**	N/A	O-FED-FEDO-160321/278
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Mar-21	7.5	A flaw was found in newlib in versions prior to 4.0.0. Improper overflow validation in the memory allocation functions mEMALIGn, pvALLOc, nano_memalign, nano_valloc, nano_pvalloc could case an integer overflow, leading to an allocation of a small buffer and then to a heap-based buffer overflow. **CVE ID : CVE-2021-3420**	https://bugzilla.redhat.com/show_bug.cgi?id=1934088	O-FED-FEDO-160321/279
gigaset					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dx600a_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Mar-21	7.8	A buffer overflow vulnerability in the AT command interface of Gigaset DX600A v41.00-175 devices allows remote attackers to force a device reboot by sending relatively long AT commands. **CVE ID : CVE-2021-25306**	N/A	O-GIG-DX60-160321/280
Improper Privilege Management	02-Mar-21	5	The telnet administrator service running on port 650 on Gigaset DX600A v41.00-175 devices does not implement any lockout or throttling functionality. This situation (together with the weak password policy that forces a 4-digit password) allows remote attackers to easily obtain administrative access via brute-force attacks. **CVE ID : CVE-2021-25309**	N/A	O-GIG-DX60-160321/281
Google					
android					
Improper Privilege Management	10-Mar-21	4.6	In getMediaOutputSliceAction of RemoteMediaSlice.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-11Android ID: A-174047735 **CVE ID : CVE-2021-0372**		
Out-of-bounds Read	10-Mar-21	2.1	In BnAudioPolicyService::onTransact of IAudioPolicyService.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169572641 **CVE ID : CVE-2021-0374**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/283
Use of Insufficiently Random Values	10-Mar-21	2.1	In onPackageModified of VoiceInteractionManagerService.java, there is a possible change of default applications due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-167261484 **CVE ID : CVE-2021-0375**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/284
Out-of-bounds Read	10-Mar-21	4.3	In getNbits of pvmp3_getbits.cpp, there is	https://source.android.co	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154076193 **CVE ID : CVE-2021-0378**	m/security/bulletin/pixel/2021-03-01	160321/285
Out-of-bounds Read	10-Mar-21	4.3	In getUpTo17bits of pvmp3_getbits.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154075955 **CVE ID : CVE-2021-0379**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/286
Incorrect Default Permissions	10-Mar-21	4.6	In onReceive of DcTracker.java, there is a possible way to trigger a provisioning URL and modify other telephony settings due to a missing permission check. This could lead to local escalation of privilege during the onboarding flow with no additional execution privileges	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172459128 **CVE ID : CVE-2021-0380**		
Incorrect Default Permissions	10-Mar-21	2.1	In updateNotifications of DeviceStorageMonitorService.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153466381 **CVE ID : CVE-2021-0381**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/288
Incorrect Default Permissions	10-Mar-21	2.1	In checkSlicePermission of SliceManagerService.java, there is a possible resource exposure due to an incorrect permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-140727941 **CVE ID : CVE-2021-0382**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/289
Improper	10-Mar-21	4.6	In done of	https://sourc	O-GOO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			CaptivePortalLoginActivity.java, there is a confused deputy. This could lead to local escalation of privilege in carrier settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-160871056 **CVE ID : CVE-2021-0383**	e.android.com/security/bulletin/pixel/2021-03-01	ANDR-160321/290
NULL Pointer Dereference	10-Mar-21	4.3	In read_and_discard_scanlines of jdapistd.c, there is a possible null pointer exception due to a missing NULL check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-173702583 **CVE ID : CVE-2021-0384**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/291
Improper Privilege Management	10-Mar-21	4.6	In createConnectToAvailableNetworkNotification of ConnectToNetworkNotificationBuilder.java, there is a possible connection to untrusted WiFi networks due to notification interaction above the lockscreen. This could lead to local escalation of	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172584372 **CVE ID : CVE-2021-0385**		
Not Available	10-Mar-21	6.8	In onCreate of UsbConfirmActivity, there is a possible tapjacking vector due to an insecure default value. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-173421110 **CVE ID : CVE-2021-0386**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/293
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	10-Mar-21	6.9	In FindQuotaDeviceForUuid of QuotaUtils.cpp, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169421939 **CVE ID : CVE-2021-0387**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	10-Mar-21	4.6	In onReceive of ImsPhoneCallTracker.java, there is a possible misattribution of data usage due to an incorrect broadcast handler. This could lead to local escalation of privilege resulting in attributing video call data to the wrong app, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-162741489 **CVE ID : CVE-2021-0388**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/295
Incorrect Default Permissions	10-Mar-21	4.6	In setNightModeActivated of UiModeManagerService.java, there is a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-168039904 **CVE ID : CVE-2021-0389**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/296
Not Available	10-Mar-21	6.8	In onCreate() of ChooseTypeAndAccountActivity.java, there is a possible way to learn the existence of an account, without permissions, due	https://source.android.com/security/bulletin/2021-03-01	O-GOO-ANDR-160321/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-172841550 **CVE ID : CVE-2021-0391**		
Double Free	10-Mar-21	4.6	In main of main.cpp, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-175124730 **CVE ID : CVE-2021-0392**	https://source.android.com/security/bulletin/2021-03-01	O-GOO-ANDR-160321/298
Out-of-bounds Write	10-Mar-21	6.8	In Scanner::LiteralBuffer::NewCapacity of scanner.cc, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution if an attacker can supply a malicious PAC file, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-	https://source.android.com/security/bulletin/2021-03-01	O-GOO-ANDR-160321/299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11 Android-8.1 Android-9 Android-10Android ID: A-168041375 **CVE ID : CVE-2021-0393**		
Out-of-bounds Read	10-Mar-21	2.1	In android_os_Parcel_readString8 of android_os_Parcel.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-172655291 **CVE ID : CVE-2021-0394**	https://source.android.com/security/bulletin/2021-03-01	O-GOO-ANDR-160321/300
Use After Free	10-Mar-21	4.6	In StopServicesAndLogViolations of reboot.cpp, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-170315126 **CVE ID : CVE-2021-0395**	https://source.android.com/security/bulletin/2021-03-01	O-GOO-ANDR-160321/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Initialization	10-Mar-21	2.1	In the Titan M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117965 **CVE ID : CVE-2021-0449**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/302
Improper Initialization	10-Mar-21	2.1	In the Titan M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117880 **CVE ID : CVE-2021-0450**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/303
Improper Initialization	10-Mar-21	2.1	In the Titan M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117871 **CVE ID : CVE-2021-0451**		
Improper Initialization	10-Mar-21	2.1	In the Titan M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117261 **CVE ID : CVE-2021-0452**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/305
Improper Initialization	10-Mar-21	2.1	In the Titan-M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117199 **CVE ID : CVE-2021-0453**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/306
Out-of-bounds Write	10-Mar-21	7.2	In the Citadel chip firmware, there is a possible out of bounds write due to a missing	https://source.android.com/security/bulletin/pixel/	O-GOO-ANDR-160321/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117047 **CVE ID : CVE-2021-0454**	2021-03-01	
Out-of-bounds Write	10-Mar-21	7.2	In the Citadel chip firmware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175116439 **CVE ID : CVE-2021-0455**	https://source.android.com/security/bulletin/pixel/2021-03-01	O-GOO-ANDR-160321/308
Not Available	09-Mar-21	4.3	Incorrect security UI in TabStrip and Navigation in Google Chrome on Android prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-21171**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	O-GOO-ANDR-160321/309
Not Available	02-Mar-21	5	Calling of non-existent provider in MobileWips application prior to SMR Feb-2021 Release 1 allows	https://security.samsungmobile.com/securityUpdate.s	O-GOO-ANDR-160321/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actions including denial of service attack by hijacking the provider. **CVE ID : CVE-2021-25330**	msb	
Improper Input Validation	04-Mar-21	4.7	Improper input check in wallpaper service in Samsung mobile devices prior to SMR Feb-2021 Release 1 allows untrusted application to cause permanent denial of service. **CVE ID : CVE-2021-25334**	https://security.samsungmobile.com, https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-160321/311
Not Available	04-Mar-21	1.9	Improper lockscreen status check in cocktailbar service in Samsung mobile devices prior to SMR Mar-2021 Release 1 allows unauthenticated users to access hidden notification contents over the lockscreen in specific condition. **CVE ID : CVE-2021-25335**	https://security.samsungmobile.com, https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-160321/312
Incorrect Authorization	04-Mar-21	4.3	Improper access control in NotificationManagerService in Samsung mobile devices prior to SMR Mar-2021 Release 1 allows untrusted applications to acquire notification access via sending a crafted malicious intent. **CVE ID : CVE-2021-25336**	https://security.samsungmobile.com, https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-160321/313
Incorrect Authorization	04-Mar-21	5.8	Improper access control in clipboard service in Samsung mobile devices prior to SMR Mar-2021	https://security.samsungmobile.com, https://secur	O-GOO-ANDR-160321/314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Release 1 allows untrusted applications to read or write certain local files. **CVE ID : CVE-2021-25337**	ity.samsungmobile.com/securityUpdate.smsb	
Incorrect Authorization	04-Mar-21	3.6	Improper memory access control in RKP in Samsung mobile devices prior to SMR Mar-2021 Release 1 allows an attacker, given a compromised kernel, to write certain part of RKP EL2 memory region. **CVE ID : CVE-2021-25338**	https://security.samsungmobile.com, https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-160321/315
Improper Input Validation	04-Mar-21	2.1	Improper address validation in HArx in Samsung mobile devices prior to SMR Mar-2021 Release 1 allows an attacker, given a compromised kernel, to corrupt EL2 memory. **CVE ID : CVE-2021-25339**	https://security.samsungmobile.com, https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-160321/316
Incorrect Authorization	04-Mar-21	2.1	Improper access control vulnerability in Samsung keyboard version prior to SMR Feb-2021 Release 1 allows physically proximate attackers to change in arbitrary settings during Initialization State. **CVE ID : CVE-2021-25340**	https://security.samsungmobile.com, https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-160321/317
Improper Authentication	04-Mar-21	2.1	Calling of non-existent provider in SMP sdk prior to version 3.0.9 allows unauthorized actions including denial of service attack by hijacking the provider.	https://security.samsungmobile.com, https://security.samsungmobile.com/serviceWeb.sms	O-GOO-ANDR-160321/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25342	b	
Improper Authentication	04-Mar-21	2.1	Calling of non-existent provider in Samsung Members prior to version 2.4.81.13 (in Android O(8.1) and below) and 3.8.00.13 (in Android P(9.0) and above) allows unauthorized actions including denial of service attack by hijacking the provider. **CVE ID : CVE-2021-25343**	https://security.samsungmobile.com/, https://security.samsungmobile.com/serviceWeb.smsb	O-GOO-ANDR-160321/319
Incorrect Default Permissions	04-Mar-21	2.1	Missing permission check in knox_custom service prior to SMR Mar-2021 Release 1 allows attackers to gain access to device's serial number without permission. **CVE ID : CVE-2021-25344**	https://security.samsungmobile.com/, https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-160321/320
Not Available	04-Mar-21	4.9	Graphic format mismatch while converting video format in hwcomposer prior to SMR Mar-2021 Release 1 results in kernel panic due to unsupported format. **CVE ID : CVE-2021-25345**	https://security.samsungmobile.com/, https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-160321/321
Out-of-bounds Write	04-Mar-21	7.5	A possible arbitrary memory overwrite vulnerabilities in quram library version prior to SMR Jan-2021 Release 1 allow arbitrary code execution. **CVE ID : CVE-2021-25346**	https://security.samsungmobile.com/, https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-160321/322
Not Available	04-Mar-21	4.6	Hijacking vulnerability in	https://secur	O-GOO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Samsung Email application version prior to SMR Feb-2021 Release 1 allows attackers to intercept when the provider is executed. **CVE ID : CVE-2021-25347**	ity.samsungmobile.com/, https://security.samsungmobile.com/securityUpdate.smsb	ANDR-160321/323
Not Available	02-Mar-21	4.6	An issue was discovered on LG mobile devices with Android OS 11 software. They mishandle fingerprint recognition because local high beam mode (LHBM) does not function properly during bright illumination. The LG ID is LVE-SMP-210001 (March 2021). **CVE ID : CVE-2021-27901**	https://lgsecurity.lge.com/	O-GOO-ANDR-160321/324
Huawei					
harmonyos					
Not Available	02-Mar-21	2.1	A component API of the HarmonyOS 2.0 has a permission bypass vulnerability. Local attackers may exploit this vulnerability to issue commands repeatedly, exhausting system service resources. **CVE ID : CVE-2021-22294**	N/A	O-HUA-HARM-160321/325
Not Available	02-Mar-21	4.9	A component of HarmonyOS 2.0 has a DoS vulnerability. Local attackers may exploit this vulnerability to mount a file system to the target device, causing DoS of the file system.	https://device.harmonyos.com/cn/console/safetyDetail?id=9145efa5d9064d94a7fc3968b6054d83&pageSize=10&pageI	O-HUA-HARM-160321/326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22296	ndex=1	
Linux					
linux_kernel					
Not Available	09-Mar-21	4.3	Inappropriate implementation in Compositing in Google Chrome on Linux and Windows prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-21178**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	O-LIN-LINU-160321/327
Use After Free	09-Mar-21	6.8	Use after free in Network Internals in Google Chrome on Linux prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21179**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	O-LIN-LINU-160321/328
Allocation of Resources Without Limits or Throttling	05-Mar-21	4.9	An issue was discovered in the Linux kernel through 5.11.3, as used with Xen PV. A certain part of the netback driver lacks necessary treatment of errors such as failed memory allocations (as a result of changes to the handling of grant mapping errors). A host OS denial of service may occur during misbehavior of a networking frontend driver. NOTE: this issue exists because of an	http://www.openwall.com/lists/oss-security/2021/03/05/1, http://xenbits.xen.org/xsa/advisory-367.html	O-LIN-LINU-160321/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			incomplete fix for CVE-2021-26931. **CVE ID : CVE-2021-28038**		
Uncontrolled Resource Consumption	05-Mar-21	2.1	An issue was discovered in the Linux kernel 5.9.x through 5.11.3, as used with Xen. In some less-common configurations, an x86 PV guest OS user can crash a Dom0 or driver domain via a large amount of I/O activity. The issue relates to misuse of guest physical addresses when a configuration has CONFIG_XEN_UNPOPULATED_ALLOC but not CONFIG_XEN_BALLOON_MEMORY_HOTPLUG. **CVE ID : CVE-2021-28039**	http://www.openwall.com/lists/oss-security/2021/03/05/2, http://xenbits.xen.org/xsa/advisory-369.html	O-LIN-LINU-160321/330
Improper Control of Generation of Code ('Code Injection')	09-Mar-21	4.6	A flaw was found in the Linux kernel in versions prior to 5.10. A violation of memory access was found while detecting a padding of int3 in the linking state. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3411**	http://blog.pi3.com.pl/?p=831	O-LIN-LINU-160321/331
Microsoft					
windows					
Use of a Broken or Risky Cryptographic	03-Mar-21	4.3	IBM Security Verify Bridge uses weaker than expected cryptographic algorithms that could allow an	https://exchange.xforce.ibmcloud.com/vulnerabilitie	O-MIC-WIND-160321/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Algorithm			attacker to decrypt highly sensitive information. IBM X-Force ID: 196617. **CVE ID : CVE-2021-20441**	s/196617, https://www.ibm.com/support/pages/node/6421023	
Use of Hard-coded Credentials	03-Mar-21	5	IBM Security Verify Bridge contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 196618. **CVE ID : CVE-2021-20442**	https://exchange.xforce.ibmcloud.com/vulnerabilities/196618, https://www.ibm.com/support/pages/node/6421025	O-MIC-WIND-160321/333
Not Available	09-Mar-21	4.3	Inappropriate implementation in Compositing in Google Chrome on Linux and Windows prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-21178**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html	O-MIC-WIND-160321/334
windows_10					
Not Available	11-Mar-21	6.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2021-26861**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26861	O-MIC-WIND-160321/335
Improper Privilege	11-Mar-21	7.2	Windows Installer Elevation of Privilege	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Vulnerability **CVE ID : CVE-2021-26862**	US/security-guidance/advisory/CVE-2021-26862	160321/336
Improper Privilege Management	11-Mar-21	7.2	Windows Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26875, CVE-2021-26900, CVE-2021-27077. **CVE ID : CVE-2021-26863**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26863	O-MIC-WIND-160321/337
Improper Privilege Management	11-Mar-21	4.6	Windows Virtual Registry Provider Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26864**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26864	O-MIC-WIND-160321/338
Improper Privilege Management	11-Mar-21	4.6	Windows Container Execution Agent Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26891. **CVE ID : CVE-2021-26865**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26865	O-MIC-WIND-160321/339
Improper Privilege Management	11-Mar-21	4.6	Windows Update Service Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26866**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26866	O-MIC-WIND-160321/340
Not Available	11-Mar-21	7.2	Windows Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2021-26867**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26867	O-MIC-WIND-160321/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-Mar-21	4.6	Windows Print Spooler Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1640. **CVE ID : CVE-2021-26878**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26878	O-MIC-WIND-160321/342
Not Available	11-Mar-21	5	Windows NAT Denial of Service Vulnerability **CVE ID : CVE-2021-26879**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26879	O-MIC-WIND-160321/343
Improper Privilege Management	11-Mar-21	4.6	Storage Spaces Controller Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26880**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26880	O-MIC-WIND-160321/344
Not Available	11-Mar-21	6.5	Microsoft Windows Media Foundation Remote Code Execution Vulnerability **CVE ID : CVE-2021-26881**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26881	O-MIC-WIND-160321/345
Improper Privilege Management	11-Mar-21	4.6	Remote Access API Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26882**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26882	O-MIC-WIND-160321/346
Exposure of Sensitive Information to an	11-Mar-21	2.1	Windows Media Photo Codec Information Disclosure Vulnerability **CVE ID : CVE-2021-26884**	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-160321/347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor				guidance/advisory/CVE-2021-26884	
Improper Privilege Management	11-Mar-21	4.6	Windows WalletService Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26871. **CVE ID : CVE-2021-26885**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26885	O-MIC-WIND-160321/348
Not Available	11-Mar-21	2.1	User Profile Service Denial of Service Vulnerability **CVE ID : CVE-2021-26886**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26886	O-MIC-WIND-160321/349
Improper Privilege Management	11-Mar-21	4.6	Microsoft Windows Folder Redirection Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26887**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26887	O-MIC-WIND-160321/350
Improper Privilege Management	11-Mar-21	4.6	Windows Update Stack Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26889**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26889	O-MIC-WIND-160321/351
Improper Control of Generation of Code ('Code Injection')	11-Mar-21	4.6	Application Virtualization Remote Code Execution Vulnerability **CVE ID : CVE-2021-26890**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26890	O-MIC-WIND-160321/352
Improper	11-Mar-21	4.6	Windows Container	https://porta	O-MIC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			Execution Agent Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26865. **CVE ID : CVE-2021-26891**	l.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26891	WIND-160321/353
Not Available	11-Mar-21	2.1	Windows Extensible Firmware Interface Security Feature Bypass Vulnerability **CVE ID : CVE-2021-26892**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26892	O-MIC-WIND-160321/354
windows_7					
Not Available	11-Mar-21	6.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2021-26861**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26861	O-MIC-WIND-160321/355
Improper Privilege Management	11-Mar-21	7.2	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26862**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26862	O-MIC-WIND-160321/356
Improper Privilege Management	11-Mar-21	4.6	Windows Print Spooler Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1640. **CVE ID : CVE-2021-26878**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26878	O-MIC-WIND-160321/357
Not Available	11-Mar-21	6.5	Microsoft Windows Media Foundation Remote Code Execution Vulnerability	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-160321/358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26881	guidance/advisory/CVE-2021-26881	
Improper Privilege Management	11-Mar-21	4.6	Remote Access API Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26882**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26882	O-MIC-WIND-160321/359
Improper Privilege Management	11-Mar-21	4.6	Microsoft Windows Folder Redirection Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26887**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26887	O-MIC-WIND-160321/360
windows_8.1					
Not Available	11-Mar-21	6.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2021-26861**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26861	O-MIC-WIND-160321/361
Improper Privilege Management	11-Mar-21	7.2	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26862**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26862	O-MIC-WIND-160321/362
Improper Privilege Management	11-Mar-21	4.6	Windows Print Spooler Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1640. **CVE ID : CVE-2021-26878**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26878	O-MIC-WIND-160321/363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	11-Mar-21	5	Windows NAT Denial of Service Vulnerability **CVE ID : CVE-2021-26879**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26879	O-MIC-WIND-160321/364
Not Available	11-Mar-21	6.5	Microsoft Windows Media Foundation Remote Code Execution Vulnerability **CVE ID : CVE-2021-26881**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26881	O-MIC-WIND-160321/365
Improper Privilege Management	11-Mar-21	4.6	Remote Access API Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26882**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26882	O-MIC-WIND-160321/366
Exposure of Sensitive Information to an Unauthorized Actor	11-Mar-21	2.1	Windows Media Photo Codec Information Disclosure Vulnerability **CVE ID : CVE-2021-26884**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26884	O-MIC-WIND-160321/367
Not Available	11-Mar-21	2.1	User Profile Service Denial of Service Vulnerability **CVE ID : CVE-2021-26886**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26886	O-MIC-WIND-160321/368
Improper Privilege Management	11-Mar-21	4.6	Microsoft Windows Folder Redirection Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26887**	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-160321/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2021-26887	
windows_rt_8.1					
Not Available	11-Mar-21	6.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2021-26861**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26861	O-MIC-WIND-160321/370
Improper Privilege Management	11-Mar-21	7.2	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26862**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26862	O-MIC-WIND-160321/371
Improper Privilege Management	11-Mar-21	4.6	Windows Print Spooler Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1640. **CVE ID : CVE-2021-26878**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26878	O-MIC-WIND-160321/372
Not Available	11-Mar-21	6.5	Microsoft Windows Media Foundation Remote Code Execution Vulnerability **CVE ID : CVE-2021-26881**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26881	O-MIC-WIND-160321/373
Improper Privilege Management	11-Mar-21	4.6	Remote Access API Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26882**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26882	O-MIC-WIND-160321/374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	11-Mar-21	2.1	Windows Media Photo Codec Information Disclosure Vulnerability **CVE ID : CVE-2021-26884**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26884	O-MIC-WIND-160321/375
Not Available	11-Mar-21	2.1	User Profile Service Denial of Service Vulnerability **CVE ID : CVE-2021-26886**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26886	O-MIC-WIND-160321/376
Improper Privilege Management	11-Mar-21	4.6	Microsoft Windows Folder Redirection Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26887**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26887	O-MIC-WIND-160321/377
windows_server_2008					
Not Available	11-Mar-21	6.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2021-26861**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26861	O-MIC-WIND-160321/378
Improper Privilege Management	11-Mar-21	7.2	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26862**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26862	O-MIC-WIND-160321/379
Improper Privilege Management	11-Mar-21	4.6	Windows Print Spooler Elevation of Privilege Vulnerability This CVE ID is	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-160321/380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2021-1640. **CVE ID : CVE-2021-26878**	US/security-guidance/advisory/CVE-2021-26878	
Not Available	11-Mar-21	6.5	Microsoft Windows Media Foundation Remote Code Execution Vulnerability **CVE ID : CVE-2021-26881**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26881	O-MIC-WIND-160321/381
Improper Privilege Management	11-Mar-21	4.6	Remote Access API Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26882**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26882	O-MIC-WIND-160321/382
Improper Privilege Management	11-Mar-21	4.6	Microsoft Windows Folder Redirection Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26887**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26887	O-MIC-WIND-160321/383
Not Available	11-Mar-21	7.5	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26877, CVE-2021-26894, CVE-2021-26895, CVE-2021-26897. **CVE ID : CVE-2021-26893**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26893	O-MIC-WIND-160321/384
Not Available	11-Mar-21	10	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26877, CVE-2021-26893, CVE-2021-26895, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-160321/385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-26897. **CVE ID : CVE-2021-26894**	2021-26894	
windows_server_2012					
Not Available	11-Mar-21	6.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2021-26861**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26861	O-MIC-WIND-160321/386
Improper Privilege Management	11-Mar-21	7.2	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26862**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26862	O-MIC-WIND-160321/387
Improper Privilege Management	11-Mar-21	4.6	Windows Print Spooler Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1640. **CVE ID : CVE-2021-26878**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26878	O-MIC-WIND-160321/388
Not Available	11-Mar-21	5	Windows NAT Denial of Service Vulnerability **CVE ID : CVE-2021-26879**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26879	O-MIC-WIND-160321/389
Not Available	11-Mar-21	6.5	Microsoft Windows Media Foundation Remote Code Execution Vulnerability **CVE ID : CVE-2021-26881**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26881	O-MIC-WIND-160321/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-Mar-21	4.6	Remote Access API Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26882**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26882	O-MIC-WIND-160321/391
Exposure of Sensitive Information to an Unauthorized Actor	11-Mar-21	2.1	Windows Media Photo Codec Information Disclosure Vulnerability **CVE ID : CVE-2021-26884**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26884	O-MIC-WIND-160321/392
Not Available	11-Mar-21	2.1	User Profile Service Denial of Service Vulnerability **CVE ID : CVE-2021-26886**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26886	O-MIC-WIND-160321/393
Improper Privilege Management	11-Mar-21	4.6	Microsoft Windows Folder Redirection Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26887**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26887	O-MIC-WIND-160321/394
Not Available	11-Mar-21	7.5	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26877, CVE-2021-26894, CVE-2021-26895, CVE-2021-26897. **CVE ID : CVE-2021-26893**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26893	O-MIC-WIND-160321/395
Not Available	11-Mar-21	10	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-160321/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2021-26877, CVE-2021-26893, CVE-2021-26895, CVE-2021-26897. **CVE ID : CVE-2021-26894**	US/security-guidance/advisory/CVE-2021-26894	
windows_server_2016					
Not Available	11-Mar-21	6.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2021-26861**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26861	O-MIC-WIND-160321/397
Improper Privilege Management	11-Mar-21	7.2	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26862**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26862	O-MIC-WIND-160321/398
Improper Privilege Management	11-Mar-21	7.2	Windows Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26875, CVE-2021-26900, CVE-2021-27077. **CVE ID : CVE-2021-26863**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26863	O-MIC-WIND-160321/399
Improper Privilege Management	11-Mar-21	4.6	Windows Virtual Registry Provider Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26864**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26864	O-MIC-WIND-160321/400
Improper Privilege Management	11-Mar-21	4.6	Windows Container Execution Agent Elevation of Privilege Vulnerability This CVE ID is unique from	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-160321/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-26891. **CVE ID : CVE-2021-26865**	guidance/advisory/CVE-2021-26865	
Improper Privilege Management	11-Mar-21	4.6	Windows Update Service Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26866**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26866	O-MIC-WIND-160321/402
Not Available	11-Mar-21	7.2	Windows Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2021-26867**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26867	O-MIC-WIND-160321/403
Improper Privilege Management	11-Mar-21	4.6	Windows Print Spooler Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1640. **CVE ID : CVE-2021-26878**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26878	O-MIC-WIND-160321/404
Not Available	11-Mar-21	5	Windows NAT Denial of Service Vulnerability **CVE ID : CVE-2021-26879**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26879	O-MIC-WIND-160321/405
Improper Privilege Management	11-Mar-21	4.6	Storage Spaces Controller Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26880**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26880	O-MIC-WIND-160321/406
Not Available	11-Mar-21	6.5	Microsoft Windows Media	https://porta	O-MIC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Foundation Remote Code Execution Vulnerability **CVE ID : CVE-2021-26881**	l.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26881	WIND-160321/407
Improper Privilege Management	11-Mar-21	4.6	Remote Access API Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26882**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26882	O-MIC-WIND-160321/408
Exposure of Sensitive Information to an Unauthorized Actor	11-Mar-21	2.1	Windows Media Photo Codec Information Disclosure Vulnerability **CVE ID : CVE-2021-26884**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26884	O-MIC-WIND-160321/409
Not Available	11-Mar-21	2.1	User Profile Service Denial of Service Vulnerability **CVE ID : CVE-2021-26886**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26886	O-MIC-WIND-160321/410
Improper Privilege Management	11-Mar-21	4.6	Microsoft Windows Folder Redirection Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26887**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26887	O-MIC-WIND-160321/411
Improper Privilege Management	11-Mar-21	4.6	Windows Update Stack Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26889**	https://portal.msrc.microsoft.com/en-US/security-guidance/adv	O-MIC-WIND-160321/412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				isory/CVE-2021-26889	
Improper Control of Generation of Code ('Code Injection')	11-Mar-21	4.6	Application Virtualization Remote Code Execution Vulnerability **CVE ID : CVE-2021-26890**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26890	O-MIC-WIND-160321/413
Improper Privilege Management	11-Mar-21	4.6	Windows Container Execution Agent Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26865. **CVE ID : CVE-2021-26891**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26891	O-MIC-WIND-160321/414
Not Available	11-Mar-21	2.1	Windows Extensible Firmware Interface Security Feature Bypass Vulnerability **CVE ID : CVE-2021-26892**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26892	O-MIC-WIND-160321/415
Not Available	11-Mar-21	7.5	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26877, CVE-2021-26894, CVE-2021-26895, CVE-2021-26897. **CVE ID : CVE-2021-26893**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26893	O-MIC-WIND-160321/416
Not Available	11-Mar-21	10	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26877, CVE-2021-26893, CVE-2021-26895, CVE-2021-26897.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26894	O-MIC-WIND-160321/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26894		
windows_server_2019					
Not Available	11-Mar-21	6.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID : CVE-2021-26861**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26861	O-MIC-WIND-160321/418
Improper Privilege Management	11-Mar-21	7.2	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26862**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26862	O-MIC-WIND-160321/419
Improper Privilege Management	11-Mar-21	7.2	Windows Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26875, CVE-2021-26900, CVE-2021-27077. **CVE ID : CVE-2021-26863**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26863	O-MIC-WIND-160321/420
Improper Privilege Management	11-Mar-21	4.6	Windows Virtual Registry Provider Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26864**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26864	O-MIC-WIND-160321/421
Improper Privilege Management	11-Mar-21	4.6	Windows Container Execution Agent Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26891. **CVE ID : CVE-2021-26865**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26865	O-MIC-WIND-160321/422
Improper	11-Mar-21	4.6	Windows Update Service	https://porta	O-MIC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26866**	l.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26866	WIND-160321/423
Improper Privilege Management	11-Mar-21	4.6	Windows Print Spooler Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1640. **CVE ID : CVE-2021-26878**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26878	O-MIC-WIND-160321/424
Not Available	11-Mar-21	5	Windows NAT Denial of Service Vulnerability **CVE ID : CVE-2021-26879**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26879	O-MIC-WIND-160321/425
Improper Privilege Management	11-Mar-21	4.6	Storage Spaces Controller Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26880**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26880	O-MIC-WIND-160321/426
Not Available	11-Mar-21	6.5	Microsoft Windows Media Foundation Remote Code Execution Vulnerability **CVE ID : CVE-2021-26881**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26881	O-MIC-WIND-160321/427
Improper Privilege Management	11-Mar-21	4.6	Remote Access API Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26882**	https://portal.msrc.microsoft.com/en-US/security-guidance/adv	O-MIC-WIND-160321/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				isory/CVE-2021-26882	
Exposure of Sensitive Information to an Unauthorized Actor	11-Mar-21	2.1	Windows Media Photo Codec Information Disclosure Vulnerability **CVE ID : CVE-2021-26884**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26884	O-MIC-WIND-160321/429
Not Available	11-Mar-21	2.1	User Profile Service Denial of Service Vulnerability **CVE ID : CVE-2021-26886**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26886	O-MIC-WIND-160321/430
Improper Privilege Management	11-Mar-21	4.6	Microsoft Windows Folder Redirection Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26887**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26887	O-MIC-WIND-160321/431
Improper Privilege Management	11-Mar-21	4.6	Windows Update Stack Elevation of Privilege Vulnerability **CVE ID : CVE-2021-26889**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26889	O-MIC-WIND-160321/432
Improper Control of Generation of Code ('Code Injection')	11-Mar-21	4.6	Application Virtualization Remote Code Execution Vulnerability **CVE ID : CVE-2021-26890**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26890	O-MIC-WIND-160321/433
Improper Privilege	11-Mar-21	4.6	Windows Container Execution Agent Elevation	https://portal.msrc.micros	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			of Privilege Vulnerability This CVE ID is unique from CVE-2021-26865. **CVE ID : CVE-2021-26891**	oft.com/en-US/security-guidance/advisory/CVE-2021-26891	160321/434
Not Available	11-Mar-21	2.1	Windows Extensible Firmware Interface Security Feature Bypass Vulnerability **CVE ID : CVE-2021-26892**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26892	O-MIC-WIND-160321/435
Not Available	11-Mar-21	7.5	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26877, CVE-2021-26894, CVE-2021-26895, CVE-2021-26897. **CVE ID : CVE-2021-26893**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26893	O-MIC-WIND-160321/436
Not Available	11-Mar-21	10	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26877, CVE-2021-26893, CVE-2021-26895, CVE-2021-26897. **CVE ID : CVE-2021-26894**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26894	O-MIC-WIND-160321/437
Redhat					
enterprise_linux_server_aus					
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short	N/A	O-RED-ENTE-160321/438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-20225**		
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-20233**	https://bugzilla.redhat.com/show_bug.cgi?id=1926263	O-RED-ENTE-160321/439
enterprise_linux_server_eus					
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data	N/A	O-RED-ENTE-160321/440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-20225**		
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-20233**	https://bugzilla.redhat.com/show_bug.cgi?id=1926263	O-RED-ENTE-160321/441
enterprise_linux_server_tus					
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	N/A	O-RED-ENTE-160321/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20225		
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-20233**	https://bugzilla.redhat.com/show_bug.cgi?id=1926263	O-RED-ENTE-160321/443
enterprise_linux_workstation					
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-20225**	N/A	O-RED-ENTE-160321/444
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06.	https://bugzilla.redhat.co	O-RED-ENTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-20233**	m/show_bug.cgi?id=1926263	160321/445
enterprise_linux					
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-20225**	N/A	O-RED-ENTE-160321/446
Out-of-bounds Write	03-Mar-21	7.2	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length	https://bugzilla.redhat.com/show_bug.cgi?id=1926263	O-RED-ENTE-160321/447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-20233**		
Use After Free	04-Mar-21	6.8	In ytnef 1.9.3, the TNEFSubjectHandler function in lib/ytnef.c allows remote attackers to cause a denial-of-service (and potentially code execution) due to a double free which can be triggered via a crafted file. **CVE ID : CVE-2021-3403**	N/A	O-RED-ENTE-160321/448
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Mar-21	6.8	In ytnef 1.9.3, the SwapWord function in lib/ytnef.c allows remote attackers to cause a denial-of-service (and potentially code execution) due to a heap buffer overflow which can be triggered via a crafted file. **CVE ID : CVE-2021-3404**	N/A	O-RED-ENTE-160321/449
Improper Control of Generation of Code ('Code	09-Mar-21	4.6	A flaw was found in the Linux kernel in versions prior to 5.10. A violation of memory access was found	http://blog.pi3.com.pl/?p=831	O-RED-ENTE-160321/450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			while detecting a padding of int3 in the linking state. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3411**		
Suse					
suse_linux_enterprise_server					
Incorrect Implementation of Authentication Algorithm	03-Mar-21	4.6	A Incorrect Implementation of Authentication Algorithm vulnerability in of SUSE SUSE Linux Enterprise Server 15 SP 3; openSUSE Tumbleweed allows local attackers to execute arbitrary code via salt without the need to specify valid credentials. This issue affects: SUSE SUSE Linux Enterprise Server 15 SP 3 salt versions prior to 3002.2-3. openSUSE Tumbleweed salt version 3002.2-2.1 and prior versions. **CVE ID : CVE-2021-25315**	https://bugzilla.suse.com/show_bug.cgi?id=1182382	O-SUS-SUSE-160321/451
XEN					
xen					
Allocation of Resources Without Limits or Throttling	05-Mar-21	4.9	An issue was discovered in the Linux kernel through 5.11.3, as used with Xen PV. A certain part of the netback driver lacks necessary treatment of errors such as failed	http://www.openwall.com/lists/oss-security/2021/03/05/1, http://xenbits.xen.org/xsa	O-XEN-XEN-160321/452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory allocations (as a result of changes to the handling of grant mapping errors). A host OS denial of service may occur during misbehavior of a networking frontend driver. NOTE: this issue exists because of an incomplete fix for CVE-2021-26931. **CVE ID : CVE-2021-28038**	/advisory-367.html	
Uncontrolled Resource Consumption	05-Mar-21	2.1	An issue was discovered in the Linux kernel 5.9.x through 5.11.3, as used with Xen. In some less-common configurations, an x86 PV guest OS user can crash a Dom0 or driver domain via a large amount of I/O activity. The issue relates to misuse of guest physical addresses when a configuration has CONFIG_XEN_UNPOPULATED_ALLOC but not CONFIG_XEN_BALLOON_MEMORY_HOTPLUG. **CVE ID : CVE-2021-28039**	http://www.openwall.com/lists/oss-security/2021/03/05/2, http://xenbits.xen.org/xsa/advisory-369.html	O-XEN-XEN-160321/453
ZTE					
zxhn_h196q_firmware					
Incorrect Authorization	05-Mar-21	2.7	A ZTE product has an information leak vulnerability. An attacker with higher authority can go beyond their authority to access files in other directories by performing specific operations,	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1014624	O-ZTE-ZXHN-160321/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in information leak. This affects: ZXHN H196Q V9.1.0C2. **CVE ID : CVE-2021-21725**		
Hardware					
gigaset					
dx600a					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Mar-21	7.8	A buffer overflow vulnerability in the AT command interface of Gigaset DX600A v41.00-175 devices allows remote attackers to force a device reboot by sending relatively long AT commands. **CVE ID : CVE-2021-25306**	N/A	H-GIG-DX60-160321/455
Improper Privilege Management	02-Mar-21	5	The telnet administrator service running on port 650 on Gigaset DX600A v41.00-175 devices does not implement any lockout or throttling functionality. This situation (together with the weak password policy that forces a 4-digit password) allows remote attackers to easily obtain administrative access via brute-force attacks. **CVE ID : CVE-2021-25309**	N/A	H-GIG-DX60-160321/456
Rockwellautomation					
compact_guardlogix_5370					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16	N/A	H-ROC-COMP-160321/457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
compact_guardlogix_5380					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with	N/A	H-ROC-COMP-160321/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
compactlogix_1768					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480:	N/A	H-ROC-COMP-160321/459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
compactlogix_1769					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34;	N/A	H-ROC-COMP-160321/460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
compactlogix_5370					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800.	N/A	H-ROC-COMP-160321/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
compactlogix_5380					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and	N/A	H-ROC-COMP-160321/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
compactlogix_5480					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an	N/A	H-ROC-COMP-160321/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
controllogix_5550					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and	N/A	H-ROC-CONT-160321/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
controllogix_5560					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380,	N/A	H-ROC-CONT-160321/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
controllogix_5570					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730,	N/A	H-ROC-CONT-160321/466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
controllogix_5580					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580;	N/A	H-ROC-CONT-160321/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SoftLogix 5800. **CVE ID : CVE-2021-22681**		
drivelogix_1794-l34					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**	N/A	H-ROC-DRIV-160321/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
drivelogix_5560					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**	N/A	H-ROC-DRIV-160321/469
drivelogix_5730					
Insufficiently Protected	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer	N/A	H-ROC-DRIV-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		160321/470
guardlogix_5570					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to	N/A	H-ROC-GUAR-160321/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
guardlogix_5580					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation	N/A	H-ROC-GUAR-160321/472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
softlogix_5800					
Insufficiently Protected Credentials	03-Mar-21	7.5	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560,	N/A	H-ROC-SOFT-160321/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. **CVE ID : CVE-2021-22681**		
Samsung					
exynos					
Not Available	04-Mar-21	4.9	Graphic format mismatch while converting video format in hwcomposer prior to SMR Mar-2021 Release 1 results in kernel panic due to unsupported format. **CVE ID : CVE-2021-25345**	https://security.samsungmobile.com/, https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-EXYN-160321/474
exynos_9830					
Incorrect Authorization	04-Mar-21	3.6	Improper memory access control in RKP in Samsung mobile devices prior to	https://security.samsungmobile.com,	H-SAM-EXYN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMR Mar-2021 Release 1 allows an attacker, given a compromised kernel, to write certain part of RKP EL2 memory region. **CVE ID : CVE-2021-25338**	https://security.samsungmobile.com/securityUpdate.smsb	160321/475
Improper Input Validation	04-Mar-21	2.1	Improper address validation in HArx in Samsung mobile devices prior to SMR Mar-2021 Release 1 allows an attacker, given a compromised kernel, to corrupt EL2 memory. **CVE ID : CVE-2021-25339**	https://security.samsungmobile.com, https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-EXYN-160321/476
ZTE					
zxhn_h196q					
Incorrect Authorization	05-Mar-21	2.7	A ZTE product has an information leak vulnerability. An attacker with higher authority can go beyond their authority to access files in other directories by performing specific operations, resulting in information leak. This affects: ZXHN H196Q V9.1.0C2. **CVE ID : CVE-2021-21725**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1014624	H-ZTE-ZXHN-160321/477