National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures(CVE) Report
01 - 15 Mar 2022 Vol. 09 No. 05

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: a3rev					
Product: page_view_count					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-03-2022	9.8	The Page View Count WordPress plugin before 2.4.15 does not sanitise and escape the post_ids parameter before using it in a SQL statement via a REST endpoint, available to both unauthenticated and authenticated users. As a result, unauthenticated attackers could perform SQL injection attacks **CVE ID : CVE-2022-0434**	N/A	A-A3R-PAGE-210322/1
Vendor: adrotate_project					
Product: adrotate					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-03-2022	7.2	The AdRotate WordPress plugin before 5.8.22 does not sanitise and escape the adrotate_action before using it in a SQL statement via the adrotate_request_action function available to	N/A	A-ADR-ADRO-210322/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admins, leading to a SQL injection **CVE ID : CVE-2022-0267**		
Vendor: adtribes					
Product: product_feed_pro_for_woocommerce					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-03-2022	5.4	The Product Feed PRO for WooCommerce WordPress plugin before 11.2.3 does not escape the rowCount parameter before outputting it back in an attribute via the woosea_categories_dropdown AJAX action (available to any authenticated user), leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-0426**	https://plugins.trac.wordpress.org/changeset/2670405	A-ADT-PROD-210322/3
Vendor: air_cargo_management_system_project					
Product: air_cargo_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-03-2022	9.8	Air Cargo Management System v1.0 was discovered to contain a SQL injection vulnerability via the ref_code parameter. **CVE ID : CVE-2022-26169**	N/A	A-AIR-AIR_-210322/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: alltube_project					
Product: alltube					
URL Redirection to Untrusted Site ('Open Redirect')	08-03-2022	6.1	alltube is an html front end for youtube-dl. On releases prior to 3.0.3, an attacker could craft a special HTML page to trigger either an open redirect attack or a Server-Side Request Forgery attack (depending on how AllTube is configured). The impact is mitigated by the fact the SSRF attack is only possible when the `stream` option is enabled in the configuration. (This option is disabled by default.) 3.0.3 contains a fix for this vulnerability. **CVE ID : CVE-2022-24739**	https://github.com/Rudloff/alltube/commit/8913f27716400dabf4906a5ad690a5238f73496a, https://github.com/Rudloff/alltube/security/advisories/GHSA-75p7-527p-w8wp, https://github.com/Rudloff/alltube/commit/3a4f09dda0a466662a4e52cde674749e0c668e8d	A-ALL-ALLT-210322/5
Vendor: Apache					
Product: any23					
Improper Restriction of XML External Entity Reference	05-03-2022	9.1	An XML external entity (XXE) injection vulnerability was discovered in the Any23 RDFa XSLTStylesheet extractor and is	https://lists.apache.org/thread/y6cm5n3ksohsrhzqknqhzy7p3mtkyk23, http://www.openwall.com/lists/oss-	A-APA-ANY2-210322/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known to affect Any23 versions < 2.7. XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem, and to interact with any back-end or external systems that the application itself can access. This issue is fixed in Apache Any23 2.7. **CVE ID : CVE-2022-25312**	security/2022/03/04/2	
Vendor: archivy_project					
Product: archivy					
URL Redirection to Untrusted Site ('Open Redirect')	06-03-2022	6.1	Open Redirect in GitHub repository archivy/archivy prior to 1.7.0. **CVE ID : CVE-2022-0697**	https://huntr.dev/bounties/2d0301a2-10ff-48f4-a346-5a0e8707835b, https://github.com/archivy/archivy/commit/2d8cb29853190d42572b36deb61127e68d6be574	A-ARC-ARCH-210322/7
Vendor: argussurveillance					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dvr					
Inadequate Encryption Strength	01-03-2022	5.5	Argus Surveillance DVR v4.0 employs weak password encryption. **CVE ID : CVE-2022-25012**	N/A	A-ARG-DVR-210322/8
Vendor: Asus					
Product: rog_live_service					
Improper Link Resolution Before File Access ('Link Following')	01-03-2022	7.7	ROG Live Service's function for deleting temp files created by installation has an improper link resolution before file access vulnerability. Since this function does not validate the path before deletion, an unauthenticated local attacker can create an unexpected symbolic link to system file path, to delete arbitrary system files and disrupt system service. **CVE ID : CVE-2022-22262**	N/A	A-ASU-ROG_-210322/9
Vendor: auto_spare_parts_management_project					
Product: auto_spare_parts_management					
Improper Neutralization of Special	02-03-2022	9.8	Auto Spare Parts Management v1.0 was discovered to contain a SQL	N/A	A-AUT-AUTO-210322/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			injection vulnerability via the user parameter. **CVE ID : CVE-2022-25398**		
Vendor: axelor					
Product: open_suite					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-03-2022	5.4	Axelor Open Suite v5.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Name parameter. **CVE ID : CVE-2022-25138**	https://forum.axelor.com/t/vuln-sur-axelor-je-suis-gentil/4768	A-AXE-OPEN-210322/11
Vendor: ayecode					
Product: userswp					
Incorrect Authorization	07-03-2022	4.3	The UsersWP WordPress plugin before 1.2.3.1 is missing access controls when updating a user avatar, and does not make sure file names for user avatars are unique, allowing a logged in user to overwrite another users avatar. **CVE ID : CVE-2022-0442**	N/A	A-AYE-USER-210322/12
Vendor: bank_management_system_project					
Product: bank_management_system					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-03-2022	9.8	Bank Management System v1.o was discovered to contain a SQL injection vulnerability via the email parameter. **CVE ID : CVE-2022-26171**	N/A	A-BAN-BANK-210322/13
Vendor: bookstackapp					
Product: bookstack					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-03-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository bookstackapp/bookstack prior to v22.02.3. **CVE ID : CVE-2022-0877**	https://github.com/bookstackapp/bookstack/commit/856fca8289b7370cafa033ea21c408e7d4303fd6, https://huntr.dev/bounties/b04df4e3-ae5a-4dc6-81ec-496248b15f3c	A-BOO-BOOK-210322/14
Vendor: Cacti					
Product: cacti					
Improper Authentication	03-03-2022	9.8	Under certain ldap conditions, Cacti authentication can be bypassed with certain credential types. **CVE ID : CVE-2022-0730**	N/A	A-CAC-CACT-210322/15
Vendor: calibre-web_project					
Product: calibre-web					
Server-Side Request	07-03-2022	9.8	Server-Side Request Forgery (SSRF) in GitHub	https://huntr.dev/bounties/7f2a5bb4-e6c7-	A-CAL-CALI-210322/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			repository janeczku/calibre-web prior to 0.6.17. **CVE ID : CVE-2022-0766**	4b6a-b8eb-face9e3add7b, https://github.com/janeczku/calibre-web/commit/965352c8d96c9eae7a6867ff76b0db137d04b0b8	
Server-Side Request Forgery (SSRF)	07-03-2022	9.9	Server-Side Request Forgery (SSRF) in GitHub repository janeczku/calibre-web prior to 0.6.17. **CVE ID : CVE-2022-0767**	https://github.com/janeczku/calibre-web/commit/965352c8d96c9eae7a6867ff76b0db137d04b0b8, https://huntr.dev/bounties/b26fc127-9b6a-4be7-a455-58aefbb62d9e	A-CAL-CALI-210322/17
Vendor: catchplugins					
Product: catch_themes_demo_import					
Unrestricted Upload of File with Dangerous Type	07-03-2022	7.2	The Catch Themes Demo Import WordPress plugin before 2.1.1 does not validate one of the file to be imported, which could allow high privivilege admin to upload an arbitrary PHP file and gain RCE even in the case of an hardened blog (ie DISALLOW_UNFILTERED_HTML, DISALLOW_FILE_EDIT and	N/A	A-CAT-CATC-210322/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DISALLOW_FILE_MODS constants set to true) **CVE ID : CVE-2022-0440**		
Vendor: cerber					
Product: wp_cerber_security\,_anti-spam_\&_malware_scan					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-03-2022	6.1	The WP Cerber Security, Anti-spam & Malware Scan WordPress plugin before 8.9.6 does not sanitise the $url variable before using it in an attribute in the Activity tab in the plugins dashboard, leading to an unauthenticated stored Cross-Site Scripting vulnerability. **CVE ID : CVE-2022-0429**	N/A	A-CER-WP_C-210322/19
Vendor: cipi					
Product: cipi					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-03-2022	5.4	Cipi 3.1.15 allows Add Server stored XSS via the /api/servers name field. **CVE ID : CVE-2022-26332**	N/A	A-CIP-CIPI-210322/20
Vendor: Codepeople					
Product: wp_time_slots_booking_form					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-03-2022	4.8	The WP Time Slots Booking Form WordPress plugin before 1.1.63 does not sanitise and escape Calendar names, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-0389**	N/A	A-COD-WP_T-210322/21
Vendor: cosmetics_and_beauty_product_online_store_project					
Product: cosmetics_and_beauty_product_online_store					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-03-2022	9.6	Cosmetics and Beauty Product Online Store v1.0 was discovered to contain multiple reflected cross-site scripting (XSS) attacks via the search parameter under the /cbpos/ app. **CVE ID : CVE-2022-25395**	N/A	A-COS-COSM-210322/22
Improper Neutralization of Special Elements used in an SQL Command	02-03-2022	9.8	Cosmetics and Beauty Product Online Store v1.0 was discovered to contain a SQL injection vulnerability via the search parameter.	N/A	A-COS-COSM-210322/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2022-25396**		
Vendor: cyberark					
Product: identity					
Use of Insufficiently Random Values	03-03-2022	5.3	CyberArk Identity versions up to and including 22.1 in the 'StartAuthentication' resource, exposes the response header 'X-CFY-TX-TM'. In certain configurations, that response header contains different, predictable value ranges which can be used to determine whether a user exists in the tenant. **CVE ID : CVE-2022-22700**	https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/ReleaseNotes/ReleaseNotes-Latest.htm	A-CYB-IDEN-210322/24
Vendor: devolutions					
Product: password_hub					
Improper Authentication	03-03-2022	6.6	The biometric lock in Devolutions Password Hub for iOS before 2021.3.4 allows attackers to access the application because of authentication bypass. An attacker must	https://devolutions.net/security/advisories/DEVO-2022-0001, https://devolutions.net/security/advisories/	A-DEV-PASS-210322/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rapidly make failed biometric authentication attempts. **CVE ID : CVE-2022-23849**		
Vendor: devowl					
Product: wordpress_real_cookie_banner					
Cross-Site Request Forgery (CSRF)	07-03-2022	6.5	The WordPress Real Cookie Banner: GDPR (DSGVO) & ePrivacy Cookie Consent WordPress plugin before 2.14.2 does not have CSRF checks in place when resetting its settings, allowing attackers to make a logged in admin reset them via a CSRF attack **CVE ID : CVE-2022-0445**	N/A	A-DEV-WORD-210322/26
Vendor: digitaldruid					
Product: hoteldruid					
Improper Control of Generation of Code ('Code Injection')	03-03-2022	8.8	HotelDruid v3.0.3 was discovered to contain a remote code execution (RCE) vulnerability which is exploited via an attacker inserting a crafted payload into the name field under the Create New Room module.	https://www.hoteldruid.com	A-DIG-HOTE-210322/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22909		
Vendor: Dolibarr					
Product: dolibarr					
Improper Control of Generation of Code ('Code Injection')	02-03-2022	8.8	Code Injection in GitHub repository dolibarr/dolibarr prior to 15.0.1. **CVE ID : CVE-2022-0819**	https://github.com/dolibarr/dolibarr/commit/2a48dd349e7de0d4a38e448b0d2ecbe25e968075, https://huntr.dev/bounties/b03d4415-d4f9-48c8-9ae2-d3aa248027b5	A-DOL-DOLI-210322/28
Vendor: dwbooster					
Product: cp_blocks					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-03-2022	4.8	The CP Blocks WordPress plugin before 1.0.15 does not sanitise and escape its "License ID" settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed. **CVE ID : CVE-2022-0448**	N/A	A-DWB-CP_B-210322/29
Vendor: e2pdf					
Product: e2pdf					
Improper Neutralization of	07-03-2022	4.8	The E2Pdf WordPress plugin before 1.16.45	https://plugins.trac.wordpress.	A-E2P-E2PD-210322/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			does not sanitise and escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2022-0535**	org/changeset/2675049/e2pdf	
Vendor: easyappointments					
Product: easyappointments					
Incorrect Authorization	09-03-2022	9.1	Exposure of Private Personal Information to an Unauthorized Actor in GitHub repository alextselegidis/easyappointments prior to 1.4.3. **CVE ID : CVE-2022-0482**	https://huntr.dev/bounties/2fe771ef-b615-45ef-9b4d-625978042e26, https://github.com/alextselegidis/easyappointments/commit/44af526a6fc5e898bc1e0132b2af9eb3a9b2c466	A-EAS-EASY-210322/31
Vendor: Elastic					
Product: kibana					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-03-2022	6.1	A cross-site-scripting (XSS) vulnerability was discovered in the Data Preview Pane (previously known as Index Pattern Preview Pane) which could allow arbitrary JavaScript to be	https://discuss.elastic.co/t/elastic-stack-7-17-1-security-update/298447	A-ELA-KIBA-210322/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed in a victim's browser. **CVE ID : CVE-2022-23710**		
Vendor: Element-it					
Product: http_commander					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-03-2022	6.1	A stored cross-site scripting (XSS) vulnerability in the admin interface in Element-IT HTTP Commander 7.0.0 allows unauthenticated users to get admin access by injecting a malicious script in the User-Agent field. **CVE ID : CVE-2022-24573**	https://www.element-it.com/news.aspx, http://element-it.com	A-ELE-HTTP-210322/33
Vendor: event_management_project					
Product: event_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-03-2022	6.1	Event Management v1.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the full_name parameter under register.php. **CVE ID : CVE-2022-25114**	N/A	A-EVE-EVEN-210322/34
Vendor: excel_streaming_reader_project					
Product: excel_streaming_reader					
Improper Restriction	02-03-2022	9.8	Excel-Streaming-Reader is an easy-	https://github.com/monitorjb	A-EXC-EXCE-210322/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of XML External Entity Reference			to-use implementation of a streaming Excel reader using Apache POI. Prior to xlsx-streamer 2.1.0, the XML parser that was used did apply all the necessary settings to prevent XML Entity Expansion issues. Upgrade to version 2.1.0 to receive a patch. There is no known workaround. **CVE ID : CVE-2022-23640**	l/excel-streaming-reader/security/advisories/GHSA-xvm2-9xvc-hx7f, https://github.com/monitorjbl/excel-streaming-reader/commit/0749c7b9709db078ccdeada16d46a34bc2910c73	
Vendor: Extensis					
Product: portfolio					
Unrestricted Upload of File with Dangerous Type	01-03-2022	8.8	Extensis Portfolio v4.0 was discovered to contain an authenticated unrestricted file upload vulnerability via the Catalog Asset Upload function. **CVE ID : CVE-2022-24251**	N/A	A-EXT-PORT-210322/36
Unrestricted Upload of File with Dangerous Type	01-03-2022	8.8	An unrestricted file upload vulnerability in the FileTransferServlet component of Extensis Portfolio v4.0 allows	N/A	A-EXT-PORT-210322/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to execute arbitrary code via a crafted file. **CVE ID : CVE-2022-24252**		
Unrestricted Upload of File with Dangerous Type	01-03-2022	8.8	Extensis Portfolio v4.0 was discovered to contain an authenticated unrestricted file upload vulnerability via the component AdminFileTransferServlet. **CVE ID : CVE-2022-24253**	N/A	A-EXT-PORT-210322/38
Unrestricted Upload of File with Dangerous Type	01-03-2022	8.8	An unrestricted file upload vulnerability in the Backup/Restore Archive component of Extensis Portfolio v4.0 allows remote attackers to execute arbitrary code via a crafted ZIP file. **CVE ID : CVE-2022-24254**	N/A	A-EXT-PORT-210322/39
Use of Hard-coded Credentials	01-03-2022	8.8	Extensis Portfolio v4.0 was discovered to contain hardcoded credentials which allows attackers to gain	N/A	A-EXT-PORT-210322/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator privileges. **CVE ID : CVE-2022-24255**		
Vendor: finastra					
Product: ssr-pages					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-03-2022	6.1	ssr-pages is an HTML page builder for the purpose of server-side rendering (SSR). In versions prior to 0.1.5, a cross site scripting (XSS) issue can occur when providing untrusted input to the `redirect.link` property as an argument to the `build(MessagePageOptions)` function. While there is no known workaround at this time, there is a patch in version 0.1.5. **CVE ID : CVE-2022-24717**	https://github.com/Finastra/ssr-pages/pull/2/commits/133606ffaec2edd9918d9fba5771ed21da7876a5, https://github.com/Finastra/ssr-pages/pull/2, https://github.com/Finastra/ssr-pages/commit/98abc59e28fec48246be0d59ac144675d6361073	A-FIN-SSR--210322/41
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-03-2022	6.5	ssr-pages is an HTML page builder for the purpose of server-side rendering (SSR). In versions prior to 0.1.4, a path traversal issue can occur when providing untrusted input to	https://github.com/Finastra/ssr-pages/pull/1, https://github.com/Finastra/ssr-pages/pull/1/commits/c3e4c563384ae3ba3892f37dd19021	A-FIN-SSR--210322/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the `svg` property as an argument to the `build(MessagePageOptions)` function. While there is no known workaround at this time, there is a patch in version 0.1.4. **CVE ID : CVE-2022-24718**	8577620780, https://github.com/Finastra/ssr-pages/security/advisories/GHSA-w6cx-qg2q-rvq8	
Vendor: fluture-node_project					
Product: fluture-node					
URL Redirection to Untrusted Site ('Open Redirect')	01-03-2022	6.1	Fluture-Node is a FP-style HTTP and streaming utils for Node based on Fluture. Using `followRedirects` or `followRedirectsWith` with any of the redirection strategies built into fluture-node 4.0.0 or 4.0.1, paired with a request that includes confidential headers such as Authorization or Cookie, exposes you to a vulnerability where, if the destination server were to redirect the request to a server on a third-party domain, or	https://github.com/fluture-js/fluture-node/commit/0c99bc511533d48be17dc6bfe641f7d0aeb34d77, https://github.com/fluture-js/fluture-node/commit/125e4474f910c1507f8ec3232848626fbc0f55c4, https://github.com/psf/requests/pull/4718	A-FLU-FLUT-210322/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the same domain over unencrypted HTTP, the headers would be included in the follow-up request and be exposed to the third party, or potential http traffic sniffing. The redirection strategies made available in version 4.0.2 automatically redact confidential headers when a redirect is followed across to another origin. A workaround has been identified by using a custom redirection strategy via the `followRedirectsWith` function. The custom strategy can be based on the new strategies available in fluture-node@4.0.2. **CVE ID : CVE-2022-24719**		
Vendor: Fortinet					
Product: fortianalyzer					
Incorrect Authorization	01-03-2022	8.8	A improper handling of insufficient permissions or privileges in	https://fortiguard.com/psirt/FG-IR-21-255	A-FOR-FORT-210322/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fortinet FortiAnalyzer version 5.6.0 through 5.6.11, FortiAnalyzer version 6.0.0 through 6.0.11, FortiAnalyzer version 6.2.0 through 6.2.9, FortiAnalyzer version 6.4.0 through 6.4.7, FortiAnalyzer version 7.0.0 through 7 .0.2, FortiManager version 5.6.0 through 5.6.11, FortiManager version 6.0.0 through 6.0.11, FortiManager version 6.2.0 through 6.2.9, FortiManager version 6.4.0 through 6.4.7, FortiManager version 7.0.0 through 7.0.2 allows attacker to bypass the device policy and force the password-change action for its user. **CVE ID : CVE-2022-22300**		
Product: fortiap-c					
Improper Neutralization of	02-03-2022	7.8	An improper neutralization of special elements	https://fortiguard.com/psirt/FG-IR-21-227	A-FOR-FORT-210322/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			used in an OS Command vulnerability [CWE-78] in FortiAP-C console 5.4.0 through 5.4.3, 5.2.0 through 5.2.1 may allow an authenticated attacker to execute unauthorized commands by running CLI commands with specifically crafted arguments. **CVE ID : CVE-2022-22301**		
Product: fortimanager					
Incorrect Authorization	01-03-2022	8.8	A improper handling of insufficient permissions or privileges in Fortinet FortiAnalyzer version 5.6.0 through 5.6.11, FortiAnalyzer version 6.0.0 through 6.0.11, FortiAnalyzer version 6.2.0 through 6.2.9, FortiAnalyzer version 6.4.0 through 6.4.7, FortiAnalyzer version 7.0.0 through 7 .0.2,	https://fortiguard.com/psirt/FG-IR-21-255	A-FOR-FORT-210322/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiManager version 5.6.0 through 5.6.11, FortiManager version 6.0.0 through 6.0.11, FortiManager version 6.2.0 through 6.2.9, FortiManager version 6.4.0 through 6.4.7, FortiManager version 7.0.0 through 7.0.2 allows attacker to bypass the device policy and force the password-change action for its user. **CVE ID : CVE-2022-22300**		
Exposure of Sensitive Information to an Unauthorized Actor	02-03-2022	5.5	An exposure of sensitive system information to an unauthorized control sphere vulnerability [CWE-497] in FortiManager versions prior to 7.0.2, 6.4.7 and 6.2.9 may allow a low privileged authenticated user to gain access to the FortiGate users credentials via the config conflict file. **CVE ID : CVE-2022-22303**	https://fortiguard.com/psirt/FG-IR-21-165	A-FOR-FORT-210322/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Foxit					
Product: pdf_editor					
NULL Pointer Dereference	10-03-2022	5.5	Foxit PDF Reader and Editor before 11.2.1 and PhantomPDF before 10.1.7 allow a NULL pointer dereference during PDF parsing because the pointer is used without proper validation. **CVE ID : CVE-2022-25108**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-210322/48
Product: pdf_reader					
NULL Pointer Dereference	10-03-2022	5.5	Foxit PDF Reader and Editor before 11.2.1 and PhantomPDF before 10.1.7 allow a NULL pointer dereference during PDF parsing because the pointer is used without proper validation. **CVE ID : CVE-2022-25108**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-210322/49
Vendor: framasoft					
Product: peertube					
Insecure Storage of Sensitive Information	09-03-2022	6.5	Insecure Storage of Sensitive Information in GitHub repository chocobozzz/peertube prior to 4.1.1.	https://github.com/chocobozzz/peertube/commit/0c058f256a195b92f124be10109c95d1f	A-FRA-PEER-210322/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0881	be93ad8, https://huntr.dev/bounties/2628431e-6a98-4063-a0e3-a8b1d9ebaa9c	
Vendor: frrouting					
Product: frrouting					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-03-2022	7.8	Buffer overflow vulnerabilities exist in FRRouting through 8.1.0 due to wrong checks on the input packet length in isisd/isis_tlvs.c. **CVE ID : CVE-2022-26125**	N/A	A-FRR-FRRO-210322/51
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-03-2022	7.8	Buffer overflow vulnerabilities exist in FRRouting through 8.1.0 due to the use of strdup with a non-zero-terminated binary string in isis_nb_notifications.c. **CVE ID : CVE-2022-26126**	N/A	A-FRR-FRRO-210322/52
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-03-2022	7.8	A buffer overflow vulnerability exists in FRRouting through 8.1.0 due to missing a check on the input packet length in the babel_packet_exa	N/A	A-FRR-FRRO-210322/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			min function in babeld/message.c. **CVE ID : CVE-2022-26127**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-03-2022	7.8	A buffer overflow vulnerability exists in FRRouting through 8.1.0 due to a wrong check on the input packet length in the babel_packet_examin function in babeld/message.c. **CVE ID : CVE-2022-26128**	N/A	A-FRR-FRRO-210322/54
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-03-2022	7.8	Buffer overflow vulnerabilities exist in FRRouting through 8.1.0 due to wrong checks on the subtlv length in the functions, parse_hello_subtlv, parse_ihu_subtlv, and parse_update_subtlv in babeld/message.c. **CVE ID : CVE-2022-26129**	N/A	A-FRR-FRRO-210322/55
Vendor: Github					
Product: viewcomponent					
Improper Neutralization of Input During	02-03-2022	6.1	VIewComponent is a framework for building view components in Ruby on Rails.	https://github.com/github/view_component/security/advisories/GHSA-	A-GIT-VIEW-210322/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Versions prior to 2.31.2 and 2.49.1 contain a cross-site scripting vulnerability that has the potential to impact anyone using translations with the view_component gem. Data received via user input and passed as an interpolation argument to the `translate` method is not properly sanitized before display. Versions 2.31.2 and 2.49.1 have been released and fully mitigate the vulnerability. As a workaround, avoid passing user input to the `translate` function, or sanitize the inputs before passing them. **CVE ID : CVE-2022-24722**	cm9w-c4rj-r2cf, https://github.com/github/view_component/commit/3f82a6e62578ff6f361aba24a1feb2caccf83ff9	
Vendor: Golang					
Product: go					
Uncontrolled Resource Consumption	05-03-2022	7.5	regexp.Compile in Go before 1.16.15 and 1.17.x before 1.17.8 allows stack exhaustion	https://groups.google.com/g/golang-announce/c/RP1hfrBYVuk	A-GOL-GO-210322/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a deeply nested expression. **CVE ID : CVE-2022-24921**		
Vendor: Haproxy					
Product: haproxy					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-03-2022	7.5	A flaw was found in the way HAProxy processed HTTP responses containing the "Set-Cookie2" header. This flaw could allow an attacker to send crafted HTTP response packets which lead to an infinite loop, eventually resulting in a denial of service condition. The highest threat from this vulnerability is availability. **CVE ID : CVE-2022-0711**	https://github.com/haproxy/haproxy/commit/bfb15ab34ead85f64cd6da0e9fb418c9cd14cee8	A-HAP-HAPR-210322/58
Vendor: hazelcast					
Product: hazelcast					
Improper Restriction of XML External Entity Reference	03-03-2022	9.8	Improper Restriction of XML External Entity Reference in GitHub repository hazelcast/hazelcast prior to 5.1. **CVE ID : CVE-2022-0265**	https://github.com/hazelcast/hazelcast/commit/4d6b666cd0291abd618c3b95cdbb51aa4208e748, https://huntr.dev/bounties/d6	A-HAZ-HAZE-210322/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				3972a2-b910-480a-a86b-d1f75d24d563	
Vendor: hestiacp					
Product: control_panel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-03-2022	6.1	Cross-site Scripting (XSS) - Generic in GitHub repository hestiacp/hestiacp prior to 1.5.9. **CVE ID : CVE-2022-0752**	https://github.com/hestiacp/hestiacp/commit/ee10e2275139684fc9a2d32169d0da702cea5ad2, https://huntr.dev/bounties/4994 0dd2-72c2-4607-857a-1fade7e8f080	A-HES-CONT-210322/60
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-03-2022	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository hestiacp/hestiacp prior to 1.5.9. **CVE ID : CVE-2022-0753**	https://github.com/hestiacp/hestiacp/commit/ee10e2275139684fc9a2d32169d0da702cea5ad2, https://huntr.dev/bounties/8ce4b776-1c53-45ec-bc5f-783077e2d324	A-HES-CONT-210322/61
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-03-2022	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository hestiacp/hestiacp prior to 1.5.10. **CVE ID : CVE-2022-0838**	https://github.com/hestiacp/hestiacp/commit/640f822d306ffb3eddf8ce2f46de75d7344283c1, https://huntr.dev/bounties/bd2fb1f1-cc8b-4ef7-8e2b-4ca686d8d614	A-HES-CONT-210322/62
Vendor: home_owners_collection_management_system_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: home_owners_collection_management_system					
Unrestricted Upload of File with Dangerous Type	02-03-2022	9.8	Home Owners Collection Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via the component /student_attendance/index.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-25016**	N/A	A-HOM-HOME-210322/63
Use of Hard-coded Credentials	02-03-2022	9.8	Home Owners Collection Management System v1.0 was discovered to contain hardcoded credentials which allows attackers to escalate privileges and access the admin panel. **CVE ID : CVE-2022-25045**	N/A	A-HOM-HOME-210322/64
Unrestricted Upload of File with Dangerous Type	02-03-2022	7.8	A remote code execution (RCE) vulnerability in the Avatar parameter under /admin/?page=user/manage_user	N/A	A-HOM-HOME-210322/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Home Owners Collection Management System v1.0 allows attackers to execute arbitrary code via a crafted PNG file. **CVE ID : CVE-2022-25115**		
Vendor: htmly					
Product: htmly					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-03-2022	5.4	A cross-site scripting (XSS) vulnerability in Htmly v2.8.1 allows attackers to excute arbitrary web scripts HTML via a crafted payload in the content field of a blog post. **CVE ID : CVE-2022-25022**	N/A	A-HTM-HTML-210322/66
Vendor: IBM					
Product: mq					
Insufficiently Protected Credentials	01-03-2022	5.5	IBM MQ Appliance 9.2 CD and 9.2 LTS local messaging users stored with a password hash that provides insufficient protection. IBM X-Force ID: 218368. **CVE ID : CVE-2022-22321**	https://exchange.xforce.ibmcloud.com/vulnerabilities/218368, https://www.ibm.com/support/pages/node/6560042	A-IBM-MQ-210322/67
Product: vios					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-03-2022	5.5	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in CAA to cause a denial of service. IBM X-Force ID: 220394. **CVE ID : CVE-2022-22350**	https://exchange.xforce.ibmcloud.com/vulnerabilities/220394, https://www.ibm.com/support/pages/node/6560390	A-IBM-VIOS-210322/68
Vendor: icegram					
Product: email_subscribers_\&_newsletters					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-03-2022	8.8	The Email Subscribers & Newsletters WordPress plugin before 5.3.2 does not correctly escape the `order` and `orderby` parameters to the `ajax_fetch_report_list` action, making it vulnerable to blind SQL injection attacks by users with roles as low as Subscriber. Further, it does not have any CSRF protection in place for the action, allowing an attacker to trick any logged in user to perform the action by clicking a link.	N/A	A-ICE-EMAI-210322/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0439		
Vendor: Icinga					
Product: icinga_web_2					
Incorrect Authorization	08-03-2022	5.3	Icinga Web 2 is an open source monitoring web interface, framework and command-line interface. Installations of Icinga 2 with the IDO writer enabled are affected. If you use service custom variables in role restrictions, and you regularly decommission service objects, users with said roles may still have access to a collection of content. Note that this only applies if a role has implicitly permitted access to hosts, due to permitted access to at least one of their services. If access to a host is permitted by other means, no sensible information has been disclosed to unauthorized users. This issue	https://github.com/Icinga/icingaweb2/security/advisories/GHSA-qcmg-vr56-x9wf, https://github.com/Icinga/icingaweb2/commit/6e989d05a1568a6733a3d912001251acc51d9293	A-ICI-ICIN-210322/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been resolved in versions 2.8.6, 2.9.6 and 2.10 of Icinga Web 2. **CVE ID : CVE-2022-24714**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-03-2022	8.8	Icinga Web 2 is an open source monitoring web interface, framework and command-line interface. Authenticated users, with access to the configuration, can create SSH resource files in unintended directories, leading to the execution of arbitrary code. This issue has been resolved in versions 2.8.6, 2.9.6 and 2.10 of Icinga Web 2. Users unable to upgrade should limit access to the Icinga Web 2 configuration. **CVE ID : CVE-2022-24715**	https://github.com/Icinga/icingaweb2/security/advisories/GHSA-v9mv-h52f-7g63, https://github.com/Icinga/icingaweb2/commit/a06d915467ca943a4b406eb9587764b8ec34cafb	A-ICI-ICIN-210322/71
Improper Limitation of a Pathname to a Restricted Directory	08-03-2022	7.5	Icinga Web 2 is an open source monitoring web interface, framework and command-line interface.	https://github.com/Icinga/icingaweb2/security/advisories/GHSA-5p3f-rh28-8frw, https://github.	A-ICI-ICIN-210322/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			Unauthenticated users can leak the contents of files of the local system accessible to the web-server user, including `icingaweb2` configuration files with database credentials. This issue has been resolved in versions 2.9.6 and 2.10 of Icinga Web 2. Database credentials should be rotated. **CVE ID : CVE-2022-24716**	com/Icinga/icingaweb2/commit/9931ed799650f5b8d5e1dc58ea3415a4cdc5773d	
Vendor: image_processing_project					
Product: image_processing					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-03-2022	9.8	image_processing is an image processing wrapper for libvips and ImageMagick/GraphicsMagick. Prior to version 1.12.2, using the `#apply` method from image_processing to apply a series of operations that are coming from unsanitized user input allows the attacker to execute shell commands. This method is called internally by	https://github.com/janko/image_processing/commit/038e4574e8f4f4b636a62394e09983c71980dada, https://github.com/janko/image_processing/security/advisories/GHSA-cxf7-qrc5-9446	A-IMA-IMAG-210322/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Active Storage variants, so Active Storage is vulnerable as well. The vulnerability has been fixed in version 1.12.2 of image_processing. As a workaround, users who process based on user input should always sanitize the user input by allowing only a constrained set of operations. **CVE ID : CVE-2022-24720**		
Vendor: jquery.cookie_project					
Product: jquery.cookie					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	02-03-2022	6.1	jQuery Cookie 1.4.1 is affected by prototype pollution, which can lead to DOM cross-site scripting (XSS). **CVE ID : CVE-2022-23395**	N/A	A-JQU-JQUE-210322/74
Vendor: keep					
Product: archeevo					
Files or Directories Accessible to External Parties	01-03-2022	7.5	Archeevo below 5.0 is affected by local file inclusion through file=~/web.config to allow an attacker to retrieve local files.	N/A	A-KEE-ARCH-210322/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23377		
Vendor: Kingsoft					
Product: wps_office					
Incorrect Default Permissions	09-03-2022	7.8	The installer of WPS Office for Windows versions prior to v11.2.0.10258 fails to configure properly the ACL for the directory where the service program is installed. **CVE ID : CVE-2022-25943**	https://www.wps.com/whatsnew/pc/20210806/	A-KIN-WPS_-210322/76
Vendor: Kofax					
Product: printix					
N/A	03-03-2022	9.8	Printix Secure Cloud Print Management through 1.3.1106.0 incorrectly uses Privileged APIs to modify values in HKEY_LOCAL_MACHINE via UITasks.PersistentRegistryData. **CVE ID : CVE-2022-25089**	https://printix.net/	A-KOF-PRIN-210322/77
Vendor: Liferay					
Product: digital_experience_platform					
Origin Validation Error	03-03-2022	5.3	The Remote App module in Liferay Portal through v7.4.3.8 and Liferay DXP	https://portal.liferay.dev/learn/security/known-vulnerabilities/	A-LIF-DIGI-210322/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through v7.4 does not check if the origin of event messages it receives matches the origin of the Remote App, allowing attackers to exfiltrate the CSRF token via a crafted event message. **CVE ID : CVE-2022-25146**	- /asset_publisher/HbL5mxmVrnXW/content/cve-2022-25146-csrf-token-exfiltration-via-remote-apps, http://liferay.com	
Product: liferay_portal					
Origin Validation Error	03-03-2022	5.3	The Remote App module in Liferay Portal through v7.4.3.8 and Liferay DXP through v7.4 does not check if the origin of event messages it receives matches the origin of the Remote App, allowing attackers to exfiltrate the CSRF token via a crafted event message. **CVE ID : CVE-2022-25146**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-25146-csrf-token-exfiltration-via-remote-apps, http://liferay.com	A-LIF-LIFE-210322/79
Vendor: Linux					
Product: linux_kernel					
N/A	09-03-2022	5.9	Microsoft Defender for Endpoint Spoofing Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	A-LIN-LINU-210322/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23278	ory/CVE-2022-23278	
Vendor: Linuxfoundation					
Product: containerd					
Exposure of Sensitive Information to an Unauthorized Actor	03-03-2022	7.5	containerd is a container runtime available as a daemon for Linux and Windows. A bug was found in containerd prior to versions 1.6.1, 1.5.10, and 1.14.12 where containers launched through containerd's CRI implementation on Linux with a specially-crafted image configuration could gain access to read-only copies of arbitrary files and directories on the host. This may bypass any policy-based enforcement on container setup (including a Kubernetes Pod Security Policy) and expose potentially sensitive information. Kubernetes and crictl can both be configured to use containerd's CRI	https://github.com/containerd/containerd/security/advisories/GHSA-crp2-qrr5-8pq7, https://github.com/containerd/containerd/releases/tag/v1.4.13, https://github.com/containerd/containerd/releases/tag/v1.6.1	A-LIN-CONT-210322/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implementation. This bug has been fixed in containerd 1.6.1, 1.5.10, and 1.4.12. Users should update to these versions to resolve the issue. **CVE ID : CVE-2022-23648**		
Vendor: marktext					
Product: marktext					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-03-2022	9.6	Mark Text v0.16.3 was discovered to contain a DOM-based cross-site scripting (XSS) vulnerability which allows attackers to perform remote code execution (RCE) via injecting a crafted payload into /lib/contentState /pasteCtrl.js. **CVE ID : CVE-2022-25069**	https://github.com/marktext/marktext/pull/3002	A-MAR-MARK-210322/82
Vendor: medical_store_management_system_project					
Product: medical_store_management_system					
Improper Neutralization of Special Elements used in an SQL Command	02-03-2022	9.8	Medical Store Management System v1.0 was discovered to contain a SQL injection vulnerability via the cid parameter	N/A	A-MED-MEDI-210322/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			under customer-add.php. **CVE ID : CVE-2022-25394**		
Vendor: mendix					
Product: forgot_password					
N/A	08-03-2022	9.8	A vulnerability has been identified in Mendix Forgot Password Appstore module (All versions >= V3.3.0 < V3.5.1). In certain configurations of the affected product, a threat actor could use the sign up flow to hijack arbitrary user accounts. **CVE ID : CVE-2022-26313**	https://cert-portal.siemens.com/productcert/pdf/ssa-134279.pdf	A-MEN-FORG-210322/84
Improper Restriction of Excessive Authentication Attempts	08-03-2022	9.8	A vulnerability has been identified in Mendix Forgot Password Appstore module (All versions >= V3.3.0 < V3.5.1), Mendix Forgot Password Appstore module (Mendix 7 compatible) (All versions < V3.2.2). Initial passwords are generated in an insecure manner. This	https://cert-portal.siemens.com/productcert/pdf/ssa-134279.pdf	A-MEN-FORG-210322/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated remote attacker to efficiently brute force passwords in specific situations. **CVE ID : CVE-2022-26314**		
Product: mendix					
Exposure of Resource to Wrong Sphere	08-03-2022	8.1	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.29), Mendix Applications using Mendix 8 (All versions < V8.18.16), Mendix Applications using Mendix 9 (All versions). If an entity has an association readable by the user, then in some cases, Mendix Runtime may not apply checks for XPath constraints that parse said associations, within apps running on affected versions. A malicious user could use this to dump and manipulate sensitive data.	https://cert-portal.siemens.com/productcert/pdf/ssa-148641.pdf	A-MEN-MEND-210322/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24309		
Exposure of Resource to Wrong Sphere	08-03-2022	6.5	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.29). When returning the result of a completed Microflow execution call the affected framework does not correctly verify, if the request was initially made by the user requesting the result. Together with predictable identifiers for Microflow execution calls, this could allow a malicious attacker to retrieve information about arbitrary Microflow execution calls made by users within the affected system. **CVE ID : CVE-2022-26317**	https://cert-portal.siemens.com/productcert/pdf/ssa-415938.pdf	A-MEN-MEND-210322/87
Vendor: metagauss					
Product: registrationmagic					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-03-2022	7.2	The RegistrationMagic WordPress plugin before 5.0.2.2 does not sanitise and escape the rm_form_id parameter before using it in a SQL statement in the Automation admin dashboard, allowing high privilege users to perform SQL injection attacks **CVE ID : CVE-2022-0420**	https://plugins.trac.wordpress.org/changeset/2672042	A-MET-REGI-210322/88
Vendor: Metalgenix					
Product: genixcms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-03-2022	5.4	In Genixcms v1.1.11, a stored Cross-Site Scripting (XSS) vulnerability exists in /gxadmin/index.php?page=themes&view=options" via the intro_title and intro_image parameters. **CVE ID : CVE-2022-24563**	https://genix.me/	A-MET-GENI-210322/89
Vendor: metaphorcreations					
Product: ditty					
Improper Neutralization of Input During	07-03-2022	6.1	The Ditty (formerly Ditty News Ticker) WordPress plugin before 3.0.15 is	https://plugins.trac.wordpress.org/changeset/2675223/ditty-news-ticker	A-MET-DITT-210322/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			affected by a Reflected Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2022-0533**		
Vendor: Microsoft					
Product: .net					
N/A	09-03-2022	7.5	.NET and Visual Studio Denial of Service Vulnerability. **CVE ID : CVE-2022-24464**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24464	A-MIC-.NET-210322/91
Product: .net_core					
N/A	09-03-2022	7.5	.NET and Visual Studio Denial of Service Vulnerability. **CVE ID : CVE-2022-24464**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24464	A-MIC-.NET-210322/92
Product: 365_apps					
N/A	09-03-2022	7.8	Microsoft Office Visio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24509, CVE-2022-24510. **CVE ID : CVE-2022-24461**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24461	A-MIC-365_-210322/93
N/A	09-03-2022	5.5	Microsoft Word Security Feature Bypass Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	A-MIC-365_-210322/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24462	ory/CVE-2022-24462	
Product: azure_site_recovery					
N/A	09-03-2022	7.2	Azure Site Recovery Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24468, CVE-2022-24470, CVE-2022-24471, CVE-2022-24517, CVE-2022-24520. **CVE ID : CVE-2022-24467**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24467	A-MIC-AZUR-210322/95
N/A	09-03-2022	7.2	Azure Site Recovery Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24467, CVE-2022-24470, CVE-2022-24471, CVE-2022-24517, CVE-2022-24520. **CVE ID : CVE-2022-24468**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24468	A-MIC-AZUR-210322/96
Improper Privilege Management	09-03-2022	8.8	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24506, CVE-2022-24515, CVE-2022-24518, CVE-2022-24519.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24469	A-MIC-AZUR-210322/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24469		
N/A	09-03-2022	7.2	Azure Site Recovery Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24467, CVE-2022-24468, CVE-2022-24471, CVE-2022-24517, CVE-2022-24520. **CVE ID : CVE-2022-24470**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24470	A-MIC-AZUR-210322/98
N/A	09-03-2022	7.2	Azure Site Recovery Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24467, CVE-2022-24468, CVE-2022-24470, CVE-2022-24517, CVE-2022-24520. **CVE ID : CVE-2022-24471**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24471	A-MIC-AZUR-210322/99
Improper Privilege Management	09-03-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24469, CVE-2022-24506, CVE-2022-24518, CVE-2022-24519. **CVE ID : CVE-2022-24515**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24515	A-MIC-AZUR-210322/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-03-2022	7.2	Azure Site Recovery Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24467, CVE-2022-24468, CVE-2022-24470, CVE-2022-24471, CVE-2022-24520. **CVE ID : CVE-2022-24517**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24517	A-MIC-AZUR-210322/101
Improper Privilege Management	09-03-2022	4.9	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24469, CVE-2022-24506, CVE-2022-24515, CVE-2022-24519. **CVE ID : CVE-2022-24518**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24518	A-MIC-AZUR-210322/102
Improper Privilege Management	09-03-2022	4.9	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24469, CVE-2022-24506, CVE-2022-24515, CVE-2022-24518. **CVE ID : CVE-2022-24519**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24519	A-MIC-AZUR-210322/103
N/A	09-03-2022	7.2	Azure Site Recovery Remote Code Execution	https://portal.msrc.microsoft.com/en-	A-MIC-AZUR-210322/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-24467, CVE-2022-24468, CVE-2022-24470, CVE-2022-24471, CVE-2022-24517. **CVE ID : CVE-2022-24520**	US/security-guidance/advisory/CVE-2022-24520	
Product: defender_for_endpoint					
N/A	09-03-2022	5.9	Microsoft Defender for Endpoint Spoofing Vulnerability. **CVE ID : CVE-2022-23278**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23278	A-MIC-DEFE-210322/105
Product: defender_for_endpoint_edr_sensor					
N/A	09-03-2022	5.9	Microsoft Defender for Endpoint Spoofing Vulnerability. **CVE ID : CVE-2022-23278**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23278	A-MIC-DEFE-210322/106
Product: defender_for_iot					
N/A	09-03-2022	8.8	Microsoft Defender for IoT Remote Code Execution Vulnerability. **CVE ID : CVE-2022-23265**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23265	A-MIC-DEFE-210322/107
Improper Privilege Management	09-03-2022	7.8	Microsoft Defender for IoT Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23266	A-MIC-DEFE-210322/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23266		
Product: exchange_server					
N/A	09-03-2022	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability. **CVE ID : CVE-2022-23277**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23277	A-MIC-EXCH-210322/109
N/A	09-03-2022	6.5	Microsoft Exchange Server Spoofing Vulnerability. **CVE ID : CVE-2022-24463**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24463	A-MIC-EXCH-210322/110
Product: heif_image_extension					
Out-of-bounds Write	09-03-2022	7.8	HEIF Image Extensions Remote Code Execution Vulnerability. **CVE ID : CVE-2022-24457**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24457	A-MIC-HEIF-210322/111
Product: hevc_video_extensions					
Out-of-bounds Write	09-03-2022	7.8	HEVC Video Extensions Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22007, CVE-2022-23301, CVE-2022-24452, CVE-2022-24453, CVE-2022-24456. **CVE ID : CVE-2022-22006**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22006	A-MIC-HEVC-210322/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	09-03-2022	7.8	HEVC Video Extensions Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22006, CVE-2022-23301, CVE-2022-24452, CVE-2022-24453, CVE-2022-24456. **CVE ID : CVE-2022-22007**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22007	A-MIC-HEVC-210322/113
N/A	09-03-2022	7.8	HEVC Video Extensions Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22006, CVE-2022-22007, CVE-2022-24452, CVE-2022-24453, CVE-2022-24456. **CVE ID : CVE-2022-23301**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23301	A-MIC-HEVC-210322/114
N/A	09-03-2022	7.8	HEVC Video Extensions Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22006, CVE-2022-22007, CVE-2022-23301, CVE-2022-24453, CVE-2022-24456. **CVE ID : CVE-2022-24452**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24452	A-MIC-HEVC-210322/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	09-03-2022	7.8	HEVC Video Extensions Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22006, CVE-2022-22007, CVE-2022-23301, CVE-2022-24452, CVE-2022-24456. **CVE ID : CVE-2022-24453**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24453	A-MIC-HEVC-210322/116
Out-of-bounds Write	09-03-2022	7.8	HEVC Video Extensions Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22006, CVE-2022-22007, CVE-2022-23301, CVE-2022-24452, CVE-2022-24453. **CVE ID : CVE-2022-24456**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24456	A-MIC-HEVC-210322/117
Product: intune_company_portal					
N/A	09-03-2022	5.5	Microsoft Intune Portal for iOS Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-24465**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24465	A-MIC-INTU-210322/118
Product: office					
N/A	09-03-2022	7.8	Microsoft Office Visio Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-OFFI-210322/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-24509, CVE-2022-24510. **CVE ID : CVE-2022-24461**	guidance/advisory/CVE-2022-24461	
N/A	09-03-2022	5.5	Microsoft Word Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-24462**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24462	A-MIC-OFFI-210322/120
Product: paint_3d					
N/A	09-03-2022	7.8	Paint 3D Remote Code Execution Vulnerability. **CVE ID : CVE-2022-23282**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23282	A-MIC-PAIN-210322/121
Product: raw_image_extension					
N/A	09-03-2022	7.8	Raw Image Extension Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-23300. **CVE ID : CVE-2022-23295**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23295	A-MIC-RAW_-210322/122
N/A	09-03-2022	7.8	Raw Image Extension Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-23295. **CVE ID : CVE-2022-23300**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23300	A-MIC-RAW_-210322/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: visual_studio_2019					
N/A	09-03-2022	7.5	.NET and Visual Studio Denial of Service Vulnerability. **CVE ID : CVE-2022-24464**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24464	A-MIC-VISU-210322/124
Product: visual_studio_2022					
N/A	09-03-2022	7.5	.NET and Visual Studio Denial of Service Vulnerability. **CVE ID : CVE-2022-24464**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24464	A-MIC-VISU-210322/125
Product: vp9_video_extensions					
N/A	09-03-2022	7.8	VP9 Video Extensions Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24501. **CVE ID : CVE-2022-24451**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24451	A-MIC-VP9_-210322/126
N/A	09-03-2022	7.8	VP9 Video Extensions Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24451. **CVE ID : CVE-2022-24501**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24501	A-MIC-VP9_-210322/127
Vendor: Microweber					
Product: microweber					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weak Password Recovery Mechanism for Forgotten Password	01-03-2022	7.5	Weak Password Recovery Mechanism for Forgotten Password in GitHub repository microweber/microweber prior to 1.3. **CVE ID : CVE-2022-0777**	https://huntr.dev/bounties/b36be8cd-544f-42bd-990d-aa1a46df44d7, https://github.com/microweber/microweber/commit/a3944cf9d1d8c41a48297ddc98302934e2511b0f	A-MIC-MICR-210322/128
Improper Control of Generation of Code ('Code Injection')	09-03-2022	8.8	Improper Neutralization of Special Elements Used in a Template Engine in GitHub repository microweber/microweber prior to 1.3. **CVE ID : CVE-2022-0896**	https://huntr.dev/bounties/113056f1-7a78-4205-9f42-940ad41d8df0, https://github.com/microweber/microweber/commit/e0224462b3dd6b1f7c6ec1197413afc6019bc3b5	A-MIC-MICR-210322/129
Product: whmcs					
Use of Incorrectly-Resolved Name or Reference	04-03-2022	6.1	Improper Resolution of Path Equivalence in GitHub repository microweber-dev/whmcs_plugin prior to 0.0.4. **CVE ID : CVE-2022-0855**	https://github.com/microweber-dev/whmcs_plugin/commit/2e7a11d332db79cc52ccda00455a15f4dc6147ff, https://huntr.dev/bounties/511879b0-cdaa-4c03-af92-deb54d46284a	A-MIC-WHMC-210322/130
Vendor: mingsoft					
Product: mcms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-03-2022	9.8	MCMS v5.2.5 was discovered to contain a SQL injection vulnerability via the categoryId parameter in the file IContentDao.xml. **CVE ID : CVE-2022-23898**	N/A	A-MIN-MCMS-210322/131
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-03-2022	9.8	MCMS v5.2.5 was discovered to contain a SQL injection vulnerability via search.do in the file /web/MCmsAction.java. **CVE ID : CVE-2022-23899**	N/A	A-MIN-MCMS-210322/132
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-03-2022	9.8	MCMS v5.2.4 was discovered to contain a SQL injection vulnerability via search.do in the file /mdiy/dict/listExcludeApp. **CVE ID : CVE-2022-25125**	N/A	A-MIN-MCMS-210322/133
Vendor: Mybb					
Product: mybb					
Improper Control of Generation of Code ('Code Injection')	09-03-2022	7.2	MyBB is a free and open source forum software. In affected versions the Admin CP's Settings	https://mybb.com/versions/1.8.30/, https://github.com/mybb/mybb/commit/92	A-MYB-MYBB-210322/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management module does not validate setting types correctly on insertion and update, making it possible to add settings of supported type `php` with PHP code, executed on on _Change Settings_ pages. This results in a Remote Code Execution (RCE) vulnerability. The vulnerable module requires Admin CP access with the `Can manage settings?` permission. MyBB's Settings module, which allows administrators to add, edit, and delete non-default settings, stores setting data in an options code string ($options_code; mybb_settings.optionscode database column) that identifies the setting type and its options, separated by a new line character (\n). In MyBB 1.2.0, support for	012b9831b330714b9f9b4646a98784113489c1, https://github.com/mybb/mybb/security/advisories/GHSA-876v-gwgh-w57f, https://www.zerodayinitiative.com/advisories/ZDI-22-503/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			setting type php was added, for which the remaining part of the options code is PHP code executed on Change Settings pages (reserved for plugins and internal use). MyBB 1.8.30 resolves this issue. There are no known workarounds. **CVE ID : CVE-2022-24734**		
Vendor: Netapp					
Product: storagegrid					
Improper Authentication	04-03-2022	4.9	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.6.0 are susceptible to a vulnerability which when successfully exploited could allow disabled, expired, or locked external user accounts to access S3 data to which they previously had access. StorageGRID 11.6.0 obtains the user account status from Active Directory or	https://security.netapp.com/advisory/NTAP-20220303-0009/	A-NET-STOR-210322/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Azure and will block S3 access for disabled user accounts during the subsequent background synchronization. User accounts that are expired or locked for Active Directory or Azure, or user accounts that are disabled, expired, or locked in identity sources other than Active Directory or Azure must be manually removed from group memberships or have their S3 keys manually removed from Tenant Manager in all versions of StorageGRID (formerly StorageGRID Webscale). **CVE ID : CVE-2022-23232**		
N/A	04-03-2022	7.5	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.6.0 are susceptible to a vulnerability which when	https://security.netapp.com/advisory/NTAP-20220303-0010/	A-NET-STOR-210322/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successfully exploited could lead to Denial of Service (DoS) of the Local Distribution Router (LDR) service. **CVE ID : CVE-2022-23233**		
Vendor: network_block_device_project					
Product: network_block_device					
Integer Overflow or Wraparound	06-03-2022	9.8	In nbd-server in nbd before 3.24, there is an integer overflow with a resultant heap-based buffer overflow. A value of 0xffffffff in the name length field will cause a zero-sized buffer to be allocated for the name, resulting in a write to a dangling pointer. This issue exists for the NBD_OPT_INFO, NBD_OPT_GO, and NBD_OPT_EXPORT_NAME messages. **CVE ID : CVE-2022-26495**	N/A	A-NET-NETW-210322/137
Out-of-bounds Write	06-03-2022	9.8	In nbd-server in nbd before 3.24, there is a stack-based buffer overflow. An attacker can cause	N/A	A-NET-NETW-210322/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a buffer overflow in the parsing of the name field by sending a crafted NBD_OPT_INFO or NBD_OPT_GO message with an large value as the length of the name. **CVE ID : CVE-2022-26496**		
Vendor: npm-lockfile_project					
Product: npm-lockfile					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-03-2022	9.8	OS Command Injection in GitHub repository ljharb/npm-lockfile in v2.0.3 and v2.0.4. **CVE ID : CVE-2022-0841**	https://github.com/ljharb/npm-lockfile/commit/bfdb84813260f0edbf759f2fde1e8c816c1478b8, https://huntr.dev/bounties/4f806dc9-2ecd-4e79-997e-5292f1bea9f1	A-NPM-NPM--210322/139
Vendor: Omron					
Product: cx-programmer					
Out-of-bounds Read	10-03-2022	7.8	Out-of-bounds read vulnerability in CX-Programmer v9.76.1 and earlier which is a part of CX-One (v4.60) suite allows an attacker to cause information disclosure and/or arbitrary code	N/A	A-OMR-CX-P-210322/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution by having a user to open a specially crafted CXP file. **CVE ID : CVE-2022-21219**		
Use After Free	10-03-2022	7.8	Use after free vulnerability in CX-Programmer v9.76.1 and earlier which is a part of CX-One (v4.60) suite allows an attacker to cause information disclosure and/or arbitrary code execution by having a user to open a specially crafted CXP file. This vulnerability is different from CVE-2022-25325. **CVE ID : CVE-2022-25230**	N/A	A-OMR-CX-P-210322/141
Out-of-bounds Write	10-03-2022	7.8	Out-of-bounds write vulnerability in CX-Programmer v9.76.1 and earlier which is a part of CX-One (v4.60) suite allows an attacker to cause information disclosure and/or arbitrary code execution by having a user to open a specially	N/A	A-OMR-CX-P-210322/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted CXP file. This vulnerability is different from CVE-2022-21124. **CVE ID : CVE-2022-25234**		
Use After Free	10-03-2022	7.8	Use after free vulnerability in CX-Programmer v9.76.1 and earlier which is a part of CX-One (v4.60) suite allows an attacker to cause information disclosure and/or arbitrary code execution by having a user to open a specially crafted CXP file. This vulnerability is different from CVE-2022-25230. **CVE ID : CVE-2022-25325**	N/A	A-OMR-CX-P-210322/143
Vendor: Open-emr					
Product: openemr					
Authorization Bypass Through User-Controlled Key	03-03-2022	8.1	An Insecure Direct Object Reference (IDOR) vulnerability in OpenEMR 6.0.0 allows any authenticated attacker to access and modify unauthorized areas via a crafted POST request to /modules/zend_m	https://www.open-emr.org/	A-OPE-OPEN-210322/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			odules/public/Installer/register. **CVE ID : CVE-2022-25471**		
Vendor: Ovirt					
Product: ovirt-engine					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	A-OVI-OVIR-210322/145
Vendor: part-db_project					
Product: part-db					
Improper Neutralization of Special Elements used in an	04-03-2022	9.8	OS Command Injection in GitHub repository part-db/part-db prior to 0.5.11.	https://huntr.dev/bounties/3e91685f-cfb9-4ee4-abaf-9b712a8fd5a6, https://github.	A-PAR-PART-210322/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			**CVE ID : CVE-2022-0848**	com/part-db/part-db/commit/9cd4eee393028aa4cab70fcbac284b0028c0bc95	
Vendor: petereport_project					
Product: petereport					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-03-2022	5.4	PeteReport Version 0.5 allows an authenticated admin user to inject persistent JavaScript code while adding an 'Attack Tree' by modifying the 'svg_file' parameter. **CVE ID : CVE-2022-23051**	N/A	A-PET-PETE-210322/147
Cross-Site Request Forgery (CSRF)	03-03-2022	6.5	PeteReport Version 0.5 contains a Cross Site Request Forgery (CSRF) vulnerability allowing an attacker to trick users into deleting users, products, reports and findings on the application. **CVE ID : CVE-2022-23052**	N/A	A-PET-PETE-210322/148
Improper Neutralization of Input During	03-03-2022	4.8	PeteReport Version 0.5 allows an authenticated admin user to inject persistent	N/A	A-PET-PETE-210322/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			JavaScript code inside the markdown descriptions while creating a product, report or finding. **CVE ID : CVE-2022-25220**		
Vendor: Phpmyadmin					
Product: phpmyadmin					
Exposure of Sensitive Information to an Unauthorized Actor	10-03-2022	7.5	PhpMyAdmin 5.1.1 and before allows an attacker to retrieve potentially sensitive information by creating invalid requests. This affects the lang parameter, the pma_parameter, and the cookie section. **CVE ID : CVE-2022-0813**	https://www.phpmyadmin.net/news/2022/2/11/phpmyadmin-4910-and-513-are-released/, https://www.incibe-cert.es/en/early-warning/security-advisories/phpmyadmin-exposure-sensitive-information	A-PHP-PHPM-210322/150
Vendor: Pimcore					
Product: pimcore					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-03-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.3.3. **CVE ID : CVE-2022-0831**	https://huntr.dev/bounties/4152e3a7-27a1-49eb-a6eb-a57506af104f, https://github.com/pimcore/pimcore/commit/e786fd44aac46febdbf916ed	A-PIM-PIMC-210322/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				6c328fbe645d80bf	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-03-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.3.3. **CVE ID : CVE-2022-0832**	https://github.com/pimcore/pimcore/commit/8ab06bfbb5a05a1b190731d9c7476ec45f5ee878, https://huntr.dev/bounties/be450b60-bc8f-4585-96a5-3c4069f1186a	A-PIM-PIMC-210322/152
Vendor: plugins-market					
Product: wp_visitor_statistics					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-03-2022	8.8	The WP Visitor Statistics (Real Time Traffic) WordPress plugin before 5.6 does not sanitise and escape the id parameter before using it in a SQL statement via the refUrlDetails AJAX action, available to any authenticated user, leading to a SQL injection **CVE ID : CVE-2022-0410**	N/A	A-PLU-WP_V-210322/153
Vendor: Pluxml					
Product: pluxml					
Improper Control of Generation of Code	01-03-2022	8.8	Pluxml v5.8.7 was discovered to allow attackers to execute arbitrary code via crafted	N/A	A-PLU-PLUX-210322/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			PHP code inserted into static pages. **CVE ID : CVE-2022-25018**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-03-2022	5.4	A cross-site scripting (XSS) vulnerability in Pluxml v5.8.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the thumbnail path of a blog post. **CVE ID : CVE-2022-25020**	N/A	A-PLU-PLUX-210322/155
Vendor: Puppet					
Product: firewall					
Improper Input Validation	02-03-2022	9.8	In certain situations it is possible for an unmanaged rule to exist on the target system that has the same comment as the rule specified in the manifest. This could allow for unmanaged rules to exist on the target system and leave the system in an unsafe state. **CVE ID : CVE-2022-0675**	https://puppet.com/security/cve/CVE-2022-0675	A-PUP-FIRE-210322/156
Vendor: pytorchlightning					
Product: pytorch_lightning					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	05-03-2022	9.8	Code Injection in GitHub repository pytorchlightning/pytorch-lightning prior to 1.6.0. **CVE ID : CVE-2022-0845**	https://huntr.dev/bounties/a795bf93-c91e-4c79-aae8-f7d8bda92e2a, https://github.com/pytorchlightning/pytorch-lightning/commit/8b7a12c52e52a06408e9231647839ddb4665e8ae	A-PYT-PYTO-210322/157
Vendor: QT					
Product: qt					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-03-2022	7.5	Qt through 5.15.8 and 6.x through 6.2.3 can load system library files from an unintended working directory. **CVE ID : CVE-2022-25634**	https://codereview.qt-project.org/c/qt/qtbase/+/396689, https://download.qt.io/official_releases/qt/6.2/CVE-2022-25643-6.2.diff, https://download.qt.io/official_releases/qt/5.15/CVE-2022-25643-5.15.diff	A-QT-QT-210322/158
Vendor: Radare					
Product: radare2					
Use After Free	05-03-2022	5.5	Use After Free in r_reg_get_name_idx in GitHub repository radareorg/radare2 prior to 5.6.6. **CVE ID : CVE-2022-0849**	https://github.com/radareorg/radare2/commit/10517e3ff0e609697eb8cde60ec8dc999ee5ea24, https://huntr.dev/bounties/29	A-RAD-RADA-210322/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				c5f76e-5f1f-43ab-a0c8-e31951e407b6	
Vendor: rdpsoft					
Product: remote_desktop_commander_suite_agent					
Unquoted Search Path or Element	03-03-2022	7.8	Remote Desktop Commander Suite Agent before v4.8 contains an unquoted service path which allows attackers to escalate privileges to the system level. **CVE ID : CVE-2022-25031**	https://www.rdpsoft.com/uqspvuln/	A-RDP-REMO-210322/160
Vendor: readymedia_project					
Product: readymedia					
Authentication Bypass by Spoofing	06-03-2022	7.4	A DNS rebinding issue in ReadyMedia (formerly MiniDLNA) before 1.3.1 allows a remote web server to exfiltrate media files. **CVE ID : CVE-2022-26505**	https://sourceforge.net/p/minidlna/git/ci/c21208508dbc131712281ec5340687e5ae89e940/	A-REA-READ-210322/161
Vendor: Redhat					
Product: codeready_linux_builder					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	A-RED-CODE-210322/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**		
Product: openshift_container_platform					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-03-2022	7.5	A flaw was found in the way HAProxy processed HTTP responses containing the "Set-Cookie2" header. This flaw could allow an attacker to send crafted HTTP response packets which lead to an infinite loop, eventually resulting in a denial of service condition. The highest threat from this vulnerability is availability.	https://github.com/haproxy/haproxy/commit/bfb15ab34ead85f64cd6da0e9fb418c9cd14cee8	A-RED-OPEN-210322/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0711		
Product: software_collections					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-03-2022	7.5	A flaw was found in the way HAProxy processed HTTP responses containing the "Set-Cookie2" header. This flaw could allow an attacker to send crafted HTTP response packets which lead to an infinite loop, eventually resulting in a denial of service condition. The highest threat from this vulnerability is availability. **CVE ID : CVE-2022-0711**	https://github.com/haproxy/haproxy/commit/bfb15ab34ead85f64cd6da0e9fb418c9cd14cee8	A-RED-SOFT-210322/164
Product: virtualization_host					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	A-RED-VIRT-210322/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**		
Vendor: rednao					
Product: smart_forms					
Missing Authorization	07-03-2022	6.5	The Smart Forms WordPress plugin before 2.6.71 does not have authorisation in its rednao_smart_forms_entries_list AJAX action, allowing any authenticated users, such as subscriber, to download arbitrary form's data, which could include sensitive information such as PII depending on the form. **CVE ID : CVE-2022-0163**	N/A	A-RED-SMAR-210322/166
Vendor: revealjs					
Product: reveal.js					
Improper Neutralizat	01-03-2022	6.1	Cross-site Scripting (XSS) -	https://github.com/hakimel/r	A-REV-REVE-210322/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			DOM in GitHub repository hakimel/reveal.js prior to 4.3.0. **CVE ID : CVE-2022-0776**	eveal.js/commit/32cdd3b1872ba8e2267c9e87ae216cb55f40f4d2, https://huntr.dev/bounties/be2b7ee4-f487-42e1-874a-6bcc410e4001	
Vendor: rtl_433_project					
Product: rlt_433					
Out-of-bounds Write	02-03-2022	5.5	rtl_433 21.12 was discovered to contain a stack overflow in the function somfy_iohc_decode(). This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted file. **CVE ID : CVE-2022-25050**	https://github.com/merbanan/rtl_433/issues/1960, https://github.com/merbanan/rtl_433/commit/2dad7b9fc67a1d0bfbe520fbd821678b8f8cc7a8	A-RTL-RLT_-210322/168
Product: rtl_433					
Off-by-one Error	02-03-2022	5.5	An Off-by-one Error occurs in cmr113_decode of rtl_433 21.12 when decoding a crafted file. **CVE ID : CVE-2022-25051**	https://github.com/merbanan/rtl_433/commit/2dad7b9fc67a1d0bfbe520fbd821678b8f8cc7a8	A-RTL-RTL_-210322/169
Vendor: salesagility					
Product: suitecrm					
Improper Neutralization of Special	07-03-2022	6.5	SQL Injection in GitHub repository	https://huntr.dev/bounties/8afb7991-c6ed-42d9-bd9b-	A-SAL-SUIT-210322/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			salesagility/suitecrm prior to 7.12.5. **CVE ID : CVE-2022-0754**	1cc83418df88, https://github.com/salesagility/suitecrm/commit/e93b269f637de313f45b32c58cef5ec012a34f58	
Improper Authentication	07-03-2022	4.3	Improper Access Control in GitHub repository salesagility/suitecrm prior to 7.12.5. **CVE ID : CVE-2022-0755**	https://github.com/salesagility/suitecrm/commit/e93b269f637de313f45b32c58cef5ec012a34f58, https://huntr.dev/bounties/cc767dbc-c676-44c1-a9d1-cd17ae77ee7e	A-SAL-SUIT-210322/171
Incorrect Authorization	07-03-2022	6.5	Improper Authorization in GitHub repository salesagility/suitecrm prior to 7.12.5. **CVE ID : CVE-2022-0756**	https://github.com/salesagility/suitecrm/commit/e93b269f637de313f45b32c58cef5ec012a34f58, https://huntr.dev/bounties/55164a63-62e4-4fb6-b4ca-87eca14f6f31	A-SAL-SUIT-210322/172
Vendor: Schneider-electric					
Product: ecostruxure_control_expert					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-03-2022	5.9	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-067-01	A-SCH-ECOS-210322/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a disruption of communication between the Modicon controller and the engineering software when an attacker is able to intercept and manipulate specific Modbus response data. Affected Product: EcoStruxure Control Expert (V15.0 SP1 and prior) **CVE ID : CVE-2022-24322**		
Improper Check for Unusual or Exceptional Conditions	09-03-2022	5.9	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause a disruption of communication between the Modicon controller and the engineering software, when an attacker is able to intercept and manipulate specific Modbus response data. Affected Product: EcoStruxure Process Expert (V2021 and prior),	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-067-01	A-SCH-ECOS-210322/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure Control Expert (V15.0 SP1 and prior) **CVE ID : CVE-2022-24323**		
Product: ecostruxure_process_expert					
Improper Check for Unusual or Exceptional Conditions	09-03-2022	5.9	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause a disruption of communication between the Modicon controller and the engineering software, when an attacker is able to intercept and manipulate specific Modbus response data. Affected Product: EcoStruxure Process Expert (V2021 and prior), EcoStruxure Control Expert (V15.0 SP1 and prior) **CVE ID : CVE-2022-24323**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-067-01	A-SCH-ECOS-210322/175
Vendor: scrapy					
Product: scrapy					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	02-03-2022	6.5	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository scrapy/scrapy prior to 2.6.1. **CVE ID : CVE-2022-0577**	https://github.com/scrapy/scrapy/commit/8ce01b3b76d4634f55067d6cfdf632ec70ba304a, https://huntr.dev/bounties/3da527b1-2348-4f69-9e88-2e11a96ac585	A-SCR-SCRA-210322/176
Vendor: seacms					
Product: seacms					
N/A	02-03-2022	9.8	seacms V11.5 is affected by an arbitrary code execution vulnerability in admin_config.php. **CVE ID : CVE-2022-23878**	N/A	A-SEA-SEAC-210322/177
Vendor: Siemens					
Product: simcenter_star-ccm\+_viewer					
Out-of-bounds Write	08-03-2022	7.8	A vulnerability has been identified in Simcenter STAR-CCM+ Viewer (All versions < V2022.1). The starview+.exe contains a memory corruption vulnerability while parsing specially crafted .SCE files. This could allow an attacker to execute code in	https://cert-portal.siemens.com/productcert/pdf/ssa-166747.pdf	A-SIE-SIMC-210322/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the context of the current process. **CVE ID : CVE-2022-24661**		
Product: sinec_network_management_syste					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-03-2022	7.2	A vulnerability has been identified in SINEC NMS (All versions). A privileged authenticated attacker could execute arbitrary commands in the local database by sending specially crafted requests to the webserver of the affected application. **CVE ID : CVE-2022-24281**	https://cert-portal.siemens.com/productcert/pdf/ssa-250085.pdf	A-SIE-SINE-210322/179
Product: sinec_network_management_system					
Deserialization of Untrusted Data	08-03-2022	7.2	A vulnerability has been identified in SINEC NMS (All versions). The affected system allows to upload JSON objects that are deserialized to Java objects. Due to insecure deserialization of user-supplied content by the affected software, a privileged attacker could exploit this	https://cert-portal.siemens.com/productcert/pdf/ssa-250085.pdf	A-SIE-SINE-210322/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a maliciously crafted serialized Java object. This could allow the attacker to execute arbitrary code on the device with root privileges. **CVE ID : CVE-2022-24282**		
Improper Privilege Management	08-03-2022	7.2	A vulnerability has been identified in SINEC NMS (All versions). The affected software do not properly check privileges between users during the same web browser session, creating an unintended sphere of control. This could allow an authenticated low privileged user to achieve privilege escalation. **CVE ID : CVE-2022-25311**	https://cert-portal.siemens.com/productcert/pdf/ssa-250085.pdf	A-SIE-SINE-210322/181
Vendor: simple_bakery_shop_management_project					
Product: simple_bakery_shop_management					
Improper Neutralization of Special Elements	02-03-2022	7.5	Simple Bakery Shop Management v1.0 was discovered to contain a SQL	N/A	A-SIM-SIMP-210322/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			injection vulnerability via the username parameter. **CVE ID : CVE-2022-25393**		
Vendor: simple_mobile_comparison_website_project					
Product: simple_mobile_comparison_website					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-03-2022	9.8	Simple Mobile Comparison Website v1.0 was discovered to contain a SQL injection vulnerability via the search parameter. **CVE ID : CVE-2022-26170**	N/A	A-SIM-SIMP-210322/183
Vendor: simple_real_estate_portal_system_project					
Product: simple_real_estate_portal_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-03-2022	9.8	Simple Real Estate Portal System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter. **CVE ID : CVE-2022-25399**	N/A	A-SIM-SIMP-210322/184
Vendor: spirit-project					
Product: spirit					
URL Redirection to Untrusted Site ('Open Redirect')	06-03-2022	6.1	Multiple Open Redirect in GitHub repository nitely/spirit prior to 0.12.3. **CVE ID : CVE-2022-0869**	https://huntr.dev/bounties/ed335a88-f68c-4e4d-ac85-f29a51b03342, https://github.com/nitely/spi	A-SPI-SPIR-210322/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				rit/commit/8f32f89654d6c30d56e0dd167059d32146fb32ef	
Vendor: stepmania					
Product: stepmania					
Exposure of Resource to Wrong Sphere	01-03-2022	9.1	The component /rootfs in RageFile of Stepmania v5.1b2 and below allows attackers access to the entire file system. **CVE ID : CVE-2022-25010**	https://github.com/stepmania/stepmania/pull/2184	A-STE-STEP-210322/186
Vendor: stripe					
Product: stripe_cli					
N/A	09-03-2022	7	Stripe CLI is a command-line tool for the Stripe eCommerce platform. A vulnerability in Stripe CLI exists on Windows when certain commands are run in a directory where an attacker has planted files. The commands are `stripe login`, `stripe config -e`, `stripe community`, and `stripe open`. MacOS and Linux are unaffected. An attacker who successfully exploits the	https://github.com/stripe/stripe-cli/commit/be38da5c0191adb77f661f769ffff2fbc7ddf6cd, https://github.com/stripe/stripe-cli/security/advisories/GHSA-4cx6-fj7j-pjx9	A-STR-STRI-210322/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can run arbitrary code in the context of the current user. The update addresses the vulnerability by throwing an error in these situations before the code can run.Users are advised to upgrade to version 1.7.13. There are no known workarounds for this issue. **CVE ID : CVE-2022-24753**		
Vendor: stylemixthemes					
Product: masterstudy_lms					
Improper Privilege Management	07-03-2022	9.8	The MasterStudy LMS WordPress plugin before 2.7.6 does to validate some parameters given when registering a new account, allowing unauthenticated users to register as an admin **CVE ID : CVE-2022-0441**	https://plugins.trac.wordpress.org/changeset/2667195	A-STY-MAST-210322/188
Vendor: Symantec					
Product: management_agent					
Improper Privilege	04-03-2022	7.8	The Symantec Management Agent is	https://support.broadcom.com/external/cont	A-SYM-MANA-210322/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			susceptible to a privilege escalation vulnerability. A low privilege local account can be elevated to the SYSTEM level through registry manipulations. **CVE ID : CVE-2022-25623**	ent/SecurityAdvisories/0/20366	
Vendor: taocms					
Product: taocms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-03-2022	7.5	An issue was discovered in taocms 3.0.2. This is a SQL blind injection that can obtain database data through the Comment Update field. **CVE ID : CVE-2022-23387**	N/A	A-TAO-TAOC-210322/190
Vendor: taogogo					
Product: taocms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-03-2022	8.8	There is a SQL injection vulnerability in the background of taocms 3.0.2 in parameter id:action=admin&id=2&ctrl=edit. **CVE ID : CVE-2022-23380**	N/A	A-TAO-TAOC-210322/191
Vendor: transloadit					
Product: uppy					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	03-03-2022	7.5	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository transloadit/uppy prior to 3.3.1. **CVE ID : CVE-2022-0528**	https://huntr.dev/bounties/8b060cc3-2420-468e-8293-b9216620175b, https://github.com/transloadit/uppy/commit/267c34045a1e62c98406d8c31261c604a11e544a	A-TRA-UPPY-210322/192
Vendor: twistedmatrix					
Product: twisted					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-03-2022	7.5	Twisted is an event-based framework for internet applications, supporting Python 3.6+. Prior to 22.2.0, Twisted SSH client and server implement is able to accept an infinite amount of data for the peer's SSH version identifier. This ends up with a buffer using all the available memory. The attach is a simple as `nc -rv localhost 22 < /dev/zero`. A patch is available in version 22.2.0. There are currently no known workarounds.	https://github.com/twisted/twisted/commit/89c395ee794e85a9657b112c4351417850330ef9, https://github.com/twisted/twisted/security/advisories/GHSA-rv6r-3f5q-9rgx, https://twistedmatrix.com/trac/ticket/10284	A-TWI-TWIS-210322/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21716		
Vendor: uri.js_project					
Product: uri.js					
URL Redirection to Untrusted Site ('Open Redirect')	06-03-2022	6.1	Open Redirect in GitHub repository medialize/uri.js prior to 1.19.10. **CVE ID : CVE-2022-0868**	https://huntr.dev/bounties/5f4db013-64bd-4a6b-9dad-870c296b0b02, https://github.com/medialize/uri.js/commit/a8166fe02f3af6dc1b2b888dcbb807155aad9509	A-URI-URI.-210322/194
Vendor: urijs_project					
Product: urijs					
Improper Input Validation	03-03-2022	5.3	URI.js is a Javascript URL mutation library. Before version 1.19.9, whitespace characters are not removed from the beginning of the protocol, so URLs are not parsed properly. This issue has been patched in version 1.19.9. Removing leading whitespace from values before passing them to URI.parse can be used as a workaround. **CVE ID : CVE-2022-24723**	https://github.com/medialize/URI.js/security/advisories/GHSA-gmv4-r438-p67f, https://github.com/medialize/uri.js/commit/86d10523a6f6e8dc4300d99d671335ee362ad316, https://huntr.dev/bounties/82ef23b8-7025-49c9-b5fc-1bb9885788e5/	A-URI-URIJ-210322/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Veritas					
Product: infoscale_operations_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-03-2022	4.8	An issue was discovered in Veritas InfoScale Operations Manager (VIOM) before 7.4.2 Patch 600 and 8.x before 8.0.0 Patch 100. A reflected cross-site scripting (XSS) vulnerability in admin/cgi-bin/listdir.pl allows authenticated remote administrators to inject arbitrary web script or HTML into an HTTP GET parameter (which reflect the user input without sanitization). **CVE ID : CVE-2022-26483**	https://www.veritas.com/content/support/en_US/security/VTS22-002	A-VER-INFO-210322/196
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-03-2022	4.9	An issue was discovered in Veritas InfoScale Operations Manager (VIOM) before 7.4.2 Patch 600 and 8.x before 8.0.0 Patch 100. The web server fails to sanitize admin/cgi-bin/rulemgr.pl/getfile/ input data,	https://www.veritas.com/content/support/en_US/security/VTS22-002	A-VER-INFO-210322/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowing a remote authenticated administrator to read arbitrary files on the system via Directory Traversal. By manipulating the resource name in GET requests referring to files with absolute paths, it is possible to access arbitrary files stored on the filesystem, including application source code, configuration files, and critical system files. **CVE ID : CVE-2022-26484**		
Vendor: victor_cms_project					
Product: victor_cms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-03-2022	9.8	Victor CMS v1.0 was discovered to contain a SQL injection vulnerability. **CVE ID : CVE-2022-26201**	N/A	A-VIC-VICT-210322/198
Vendor: Videousermanuals					
Product: white_label_cms					
Improper Neutralization of	07-03-2022	6.1	The White Label CMS WordPress plugin before	https://plugins.trac.wordpress.	A-VID-WHIT-210322/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			2.2.9 does not sanitise and validate the wlcms[_login_custom_js] parameter before outputting it back in the response while previewing, leading to a Reflected Cross-Site Scripting issue **CVE ID : CVE-2022-0422**	org/changeset/2672615	
Vendor: video_conferencing_with_zoom_project					
Product: video_conferencing_with_zoom					
N/A	07-03-2022	4.3	The Video Conferencing with Zoom WordPress plugin before 3.8.17 does not have authorisation in its vczapi_get_wp_users AJAX action, allowing any authenticated users, such as subscriber to download the list of email addresses registered on the blog **CVE ID : CVE-2022-0384**	https://plugins.trac.wordpress.org/changeset/2671219	A-VID-VIDE-210322/200
Vendor: Vmware					
Product: workspace_one_boxer					
Improper Neutralizat	02-03-2022	5.4	VMware Workspace ONE	https://www.vmware.com/sec	A-VMW-WORK-210322/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Boxer contains a stored cross-site scripting (XSS) vulnerability. Due to insufficient sanitization and validation, in VMware Workspace ONE Boxer calendar event descriptions, a malicious actor can inject script tags to execute arbitrary script within a user's window. **CVE ID : CVE-2022-22944**	urity/advisories/VMSA-2022-0006.html	
Vendor: Weblate					
Product: weblate					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	04-03-2022	8.8	The package weblate from 0 and before 4.11.1 are vulnerable to Remote Code Execution (RCE) via argument injection when using git or mercurial repositories. Authenticated users, can change the behavior of the application in an unintended way, leading to command execution.	https://snyk.io/vuln/SNYK-PYTHON-WEBLATE-2414088, https://github.com/WeblateOrg/weblate/pull/7338, https://github.com/WeblateOrg/weblate/pull/7337, https://github.com/WeblateOrg/weblate/releases/tag/weblate-4.11.1	A-WEB-WEBL-210322/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23915		
Vendor: Webmin					
Product: webmin					
Incorrect Authorization	02-03-2022	8.8	Improper Access Control to Remote Code Execution in GitHub repository webmin/webmin prior to 1.990. **CVE ID : CVE-2022-0824**	https://github.com/webmin/webmin/commit/39ea464f0c40b325decd6a5bfb7833fa4a142e38, https://huntr.dev/bounties/d0049a96-de90-4b1a-9111-94de1044f295	A-WEB-WEBM-210322/203
Incorrect Authorization	02-03-2022	8.1	Improper Authorization in GitHub repository webmin/webmin prior to 1.990. **CVE ID : CVE-2022-0829**	https://huntr.dev/bounties/f2d0389f-d7d1-4f34-9f9d-268b0a0da05e, https://github.com/webmin/webmin/commit/eeeea3c097f5cc473770119f7ac61f1dcfa671b9	A-WEB-WEBM-210322/204
Vendor: wpbrigade					
Product: loginpress					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-03-2022	6.1	The LoginPress | Custom Login Page Customizer WordPress plugin before 1.5.12 does not escape the redirect-page parameter before outputting it back in an attribute, leading to a	N/A	A-WPB-LOGI-210322/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Reflected Cross-Site Scripting **CVE ID : CVE-2022-0347**		
Vendor: wpdeveloper					
Product: notificationx					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-03-2022	9.8	The NotificationX WordPress plugin before 2.3.9 does not sanitise and escape the nx_id parameter before using it in a SQL statement, leading to an Unauthenticated Blind SQL Injection **CVE ID : CVE-2022-0349**	N/A	A-WPD-NOTI-210322/206
Vendor: yop-poll					
Product: yop-poll					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-03-2022	5.4	The YOP Poll WordPress plugin before 6.3.5 does not sanitise and escape some of the settings (available to users with a role as low as author) before outputting them, leading to a Stored Cross-Site Scripting issue **CVE ID : CVE-2022-0205**	N/A	A-YOP-YOP--210322/207
Vendor: Zohocorp					
Product: manageengine_desktop_central					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	02-03-2022	5.3	Zoho ManageEngine Desktop Central before 10.1.2137.8 exposes the installed server name to anyone. The internal hostname can be discovered by reading HTTP redirect responses. **CVE ID : CVE-2022-23779**	https://www.manageengine.com/products/desktop-central/cve-2022-23779.html	A-ZOH-MANA-210322/208
Product: manageengine_key_manager_plus					
Exposure of Resource to Wrong Sphere	01-03-2022	4.3	An issue was discovered in Zoho ManageEngine Key Manager Plus 6.1.6. A user, with the level Operator, can see all SSH servers (and user information) even if no SSH server or user is associated to the operator. **CVE ID : CVE-2022-24446**	https://www.manageengine.com/key-manager/release-notes.html#6200	A-ZOH-MANA-210322/209
Exposure of Sensitive Information to an Unauthorized Actor	02-03-2022	6.5	An issue was discovered in Zoho ManageEngine Key Manager Plus before 6200. A service exposed by the application allows a user, with the level Operator,	https://www.manageengine.com/key-manager/release-notes.html#6200	A-ZOH-MANA-210322/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access stored SSL certificates and associated key pairs during export. **CVE ID : CVE-2022-24447**		
Product: manageengine_sharepoint_manager_plus					
Improper Privilege Management	02-03-2022	9.8	Zoho ManageEngine SharePoint Manager Plus before 4329 is vulnerable to a sensitive data leak that leads to privilege escalation. **CVE ID : CVE-2022-24305**	https://www.manageengine.com/sharepoint-management-reporting/release-notes.html#4329	A-ZOH-MANA-210322/211
Incorrect Authorization	02-03-2022	9.8	Zoho ManageEngine SharePoint Manager Plus before 4329 allows account takeover because authorization is mishandled. **CVE ID : CVE-2022-24306**	https://www.manageengine.com/sharepoint-management-reporting/release-notes.html#4329	A-ZOH-MANA-210322/212
Vendor: Zulip					
Product: zulip_server					
Improper Neutralization of Input During Web Page Generation	02-03-2022	5.4	Zulip is an open source team chat app. The `main` development branch of Zulip Server from June 2021 and later is vulnerable to a	https://github.com/zulip/zulip/security/advisories/GHSA-fc77-h3jc-6mfv, https://github.com/zulip/zulip/commit/e09	A-ZUL-ZULI-210322/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			cross-site scripting vulnerability on the recent topics page. An attacker could maliciously craft a full name for their account and send messages to a topic with several participants; a victim who then opens an overflow tooltip including this full name on the recent topics page could trigger execution of JavaScript code controlled by the attacker. Users running a Zulip server from the main branch should upgrade from main (2022-03-01 or later) again to deploy this fix. **CVE ID : CVE-2022-23656**	0027adcbf62737d5b1f83a9618a9500a49321	
Hardware					
Vendor: Dlink					
Product: dir-859					
Out-of-bounds Write	04-03-2022	5.5	D-Link DIR-859 v1.05 was discovered to contain a stack-based buffer overflow via the function	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/	H-DLI-DIR--210322/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			genacgi_main. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2022-25106**	publication.aspx?name=SAP10267	
Product: dir-859_a3					
Out-of-bounds Write	04-03-2022	5.5	D-Link DIR-859 v1.05 was discovered to contain a stack-based buffer overflow via the function genacgi_main. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2022-25106**	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10267	H-DLI-DIR--210322/215
Vendor: HP					
Product: probook_440_g8					
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23953**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	H-HP-PROB-210322/216
N/A	02-03-2022	5.5	Potential vulnerabilities have been	https://support.hp.com/us-en/document/i	H-HP-PROB-210322/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23954**	sh_5818692-5818718-16	
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23955**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	H-HP-PROB-210322/218
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23956**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	H-HP-PROB-210322/219
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23957**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	H-HP-PROB-210322/220
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the	https://support.hp.com/us-en/document/i	H-HP-PROB-210322/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23958**	sh_5818692-5818718-16	
Product: prodesk_405_g6_small_form_factor					
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23953**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	H-HP-PROD-210322/222
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23954**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	H-HP-PROD-210322/223
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23955**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	H-HP-PROD-210322/224
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the	https://support.hp.com/us-en/document/i	H-HP-PROD-210322/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23956**	sh_5818692-5818718-16	
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23957**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	H-HP-PROD-210322/226
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23958**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	H-HP-PROD-210322/227
Vendor: Siemens					
Product: sinumerik_mc					
Improper Privilege Management	08-03-2022	7.8	A vulnerability has been identified in SINUMERIK MC (All versions < V1.15 SP1), SINUMERIK ONE (All versions < V6.15 SP1). The sc SUID binary on affected devices provides several commands that	https://cert-portal.siemens.com/productcert/pdf/ssa-337210.pdf	H-SIE-SINU-210322/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are used to execute system commands or modify system files. A specific set of operations using sc could allow local attackers to escalate their privileges to root. **CVE ID : CVE-2022-24408**		
Product: sinumerik_one					
Improper Privilege Management	08-03-2022	7.8	A vulnerability has been identified in SINUMERIK MC (All versions < V1.15 SP1), SINUMERIK ONE (All versions < V6.15 SP1). The sc SUID binary on affected devices provides several commands that are used to execute system commands or modify system files. A specific set of operations using sc could allow local attackers to escalate their privileges to root. **CVE ID : CVE-2022-24408**	https://cert-portal.siemens.com/productcert/pdf/ssa-337210.pdf	H-SIE-SINU-210322/229
Vendor: Tenda					
Product: ax1806					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsUser parameter. **CVE ID : CVE-2022-25546**	N/A	H-TEN-AX18-210322/230
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the time parameter. **CVE ID : CVE-2022-25547**	N/A	H-TEN-AX18-210322/231
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the	N/A	H-TEN-AX18-210322/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			serverName parameter. **CVE ID : CVE-2022-25548**		
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsEn parameter. **CVE ID : CVE-2022-25549**	N/A	H-TEN-AX18-210322/233
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the deviceName parameter. **CVE ID : CVE-2022-25550**	N/A	H-TEN-AX18-210322/234
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the	N/A	H-TEN-AX18-210322/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsDomain parameter. **CVE ID : CVE-2022-25551**		
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function form_fast_setting_wifi_set. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ssid parameter. **CVE ID : CVE-2022-25552**	N/A	H-TEN-AX18-210322/236
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsPwd parameter.	N/A	H-TEN-AX18-210322/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25553		
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the deviceId parameter. **CVE ID : CVE-2022-25554**	N/A	H-TEN-AX18-210322/238
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ntpServer parameter. **CVE ID : CVE-2022-25555**	N/A	H-TEN-AX18-210322/239
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a heap overflow in the function saveParentControlInfo. This vulnerability	N/A	H-TEN-AX18-210322/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to cause a Denial of Service (DoS) via the urls parameter. **CVE ID : CVE-2022-25557**		
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetProvince. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ProvinceCode parameter. **CVE ID : CVE-2022-25558**	N/A	H-TEN-AX18-210322/241
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the time parameter. **CVE ID : CVE-2022-25566**	N/A	H-TEN-AX18-210322/242
Operating System					
Vendor: Apple					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: macos					
N/A	09-03-2022	5.9	Microsoft Defender for Endpoint Spoofing Vulnerability. **CVE ID : CVE-2022-23278**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23278	O-APP-MACO-210322/243
Vendor: Debian					
Product: debian_linux					
Integer Overflow or Wraparound	06-03-2022	9.8	In nbd-server in nbd before 3.24, there is an integer overflow with a resultant heap-based buffer overflow. A value of 0xffffffff in the name length field will cause a zero-sized buffer to be allocated for the name, resulting in a write to a dangling pointer. This issue exists for the NBD_OPT_INFO, NBD_OPT_GO, and NBD_OPT_EXPORT_NAME messages. **CVE ID : CVE-2022-26495**	N/A	O-DEB-DEBI-210322/244
Vendor: Dlink					
Product: dir-859_a3_firmware					
Out-of-bounds Write	04-03-2022	5.5	D-Link DIR-859 v1.05 was discovered to contain a stack-based buffer	https://www.dlink.com/en/security-bulletin/, https://support announcement.	O-DLI-DIR--210322/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the function genacgi_main. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2022-25106**	us.dlink.com/announcement/publication.aspx?name=SAP10267	
Product: dir-859_firmware					
Out-of-bounds Write	04-03-2022	5.5	D-Link DIR-859 v1.05 was discovered to contain a stack-based buffer overflow via the function genacgi_main. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2022-25106**	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10267	O-DLI-DIR--210322/246
Vendor: espruino					
Product: espruino					
Out-of-bounds Write	05-03-2022	7.8	Espruino 2v11.251 was discovered to contain a stack buffer overflow via src/jsvar.c in jsvNewFromString. **CVE ID : CVE-2022-25044**	https://github.com/espruino/Espruino/commit/e069be2ecc5060ef47391716e4de94999595b260, https://github.com/espruino/Espruino/issues/2142	O-ESP-ESPR-210322/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-03-2022	7.8	Espruino 2v11 release was discovered to contain a stack buffer overflow via src/jsvar.c in jsvGetNextSibling. **CVE ID : CVE-2022-25465**	N/A	O-ESP-ESPR-210322/248
Vendor: Fedoraproject					
Product: fedora					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-FED-FEDO-210322/249
Vendor: Google					
Product: android					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-03-2022	5.9	Microsoft Defender for Endpoint Spoofing Vulnerability. **CVE ID : CVE-2022-23278**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23278	O-GOO-ANDR-210322/250
Improper Authentication	04-03-2022	7.8	When the device is in factory state, it can be access the shell without adb authentication process. The LG ID is LVE-SMP-210010. **CVE ID : CVE-2022-23729**	https://lgsecurity.lge.com/bulletins/mobile	O-GOO-ANDR-210322/251
Vendor: HP					
Product: probook_440_g8_firmware					
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23953**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	O-HP-PROB-210322/252
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23954**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	O-HP-PROB-210322/253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23955**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	O-HP-PROB-210322/254
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23956**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	O-HP-PROB-210322/255
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23957**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	O-HP-PROB-210322/256
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23958**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	O-HP-PROB-210322/257
Product: prodesk_405_g6_small_form_factor_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23953**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	O-HP-PROD-210322/258
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23954**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	O-HP-PROD-210322/259
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23955**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	O-HP-PROD-210322/260
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23956**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	O-HP-PROD-210322/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23957**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	O-HP-PROD-210322/262
N/A	02-03-2022	5.5	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service. **CVE ID : CVE-2022-23958**	https://support.hp.com/us-en/document/ish_5818692-5818718-16	O-HP-PROD-210322/263
Vendor: IBM					
Product: aix					
N/A	02-03-2022	5.5	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in CAA to cause a denial of service. IBM X-Force ID: 220394. **CVE ID : CVE-2022-22350**	https://exchange.xforce.ibmcloud.com/vulnerabilities/220394, https://www.ibm.com/support/pages/node/6560390	O-IBM-AIX-210322/264
Vendor: icewale					
Product: casaos					
Improper Neutralization of Special Elements	10-03-2022	9.8	CasaOS before v0.2.7 was discovered to contain a command	https://github.com/IceWhaleTech/CasaOS/commit/d060968b7ab08e7f8cb	O-ICE-CASA-210322/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			injection vulnerability via the component leave or join zerotier api. **CVE ID : CVE-2022-24193**	fe7ca9ccdfa47afe9bb06	
Vendor: Linux					
Product: linux_kernel					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-LIN-LINU-210322/266
Buffer Copy without Checking Size of Input	06-03-2022	7.8	st21nfca_connectivity_event_received in drivers/nfc/st21nfca/se.c in the Linux kernel	https://github.com/torvalds/linux/commit/4fbcc1a4cb20fe26ad0225679c536c80f1648221	O-LIN-LINU-210322/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			through 5.16.12 has EVT_TRANSACTION buffer overflows because of untrusted length parameters. **CVE ID : CVE-2022-26490**		
Vendor: Microsoft					
Product: windows					
N/A	09-03-2022	7	Stripe CLI is a command-line tool for the Stripe eCommerce platform. A vulnerability in Stripe CLI exists on Windows when certain commands are run in a directory where an attacker has planted files. The commands are `stripe login`, `stripe config -e`, `stripe community`, and `stripe open`. MacOS and Linux are unaffected. An attacker who successfully exploits the vulnerability can run arbitrary code in the context of the current user. The update addresses the vulnerability by	https://github.com/stripe/stripe-cli/commit/be38da5c0191adb77f661f769ffff2fbc7ddf6cd, https://github.com/stripe/stripe-cli/security/advisories/GHSA-4cx6-fj7j-pjx9	O-MIC-WIND-210322/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			throwing an error in these situations before the code can run.Users are advised to upgrade to version 1.7.13. There are no known workarounds for this issue. **CVE ID : CVE-2022-24753**		
NULL Pointer Dereference	10-03-2022	5.5	Foxit PDF Reader and Editor before 11.2.1 and PhantomPDF before 10.1.7 allow a NULL pointer dereference during PDF parsing because the pointer is used without proper validation. **CVE ID : CVE-2022-25108**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-210322/269
Product: windows_10					
Improper Privilege Management	09-03-2022	7	Xbox Live Auth Manager for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21967**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21967	O-MIC-WIND-210322/270
Concurrent Execution using Shared Resource	09-03-2022	4.7	Windows Hyper-V Denial of Service Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			**CVE ID : CVE-2022-21975**	ory/CVE-2022-21975	
N/A	09-03-2022	3.3	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-22010. **CVE ID : CVE-2022-21977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21977	O-MIC-WIND-210322/272
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-23285. **CVE ID : CVE-2022-21990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21990	O-MIC-WIND-210322/273
N/A	09-03-2022	5.5	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-21977. **CVE ID : CVE-2022-22010**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22010	O-MIC-WIND-210322/274
N/A	09-03-2022	6.5	Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-23253**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23253	O-MIC-WIND-210322/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-03-2022	5.9	Microsoft Defender for Endpoint Spoofing Vulnerability. **CVE ID : CVE-2022-23278**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23278	O-MIC-WIND-210322/276
N/A	09-03-2022	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23281**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23281	O-MIC-WIND-210322/277
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23287, CVE-2022-24505. **CVE ID : CVE-2022-23283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23283	O-MIC-WIND-210322/278
Improper Privilege Management	09-03-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23284**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23284	O-MIC-WIND-210322/279
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21990. **CVE ID : CVE-2022-23285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23285	O-MIC-WIND-210322/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-03-2022	7	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23286**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23286	O-MIC-WIND-210322/281
Improper Privilege Management	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23283, CVE-2022-24505. **CVE ID : CVE-2022-23287**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23287	O-MIC-WIND-210322/282
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows DWM Core Library Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23291. **CVE ID : CVE-2022-23288**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23288	O-MIC-WIND-210322/283
Improper Privilege Management	09-03-2022	7.8	Windows Inking COM Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23290**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23290	O-MIC-WIND-210322/284
Improper Privilege Management	09-03-2022	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23291	O-MIC-WIND-210322/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-23288. **CVE ID : CVE-2022-23291**		
Improper Privilege Management	09-03-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23293**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23293	O-MIC-WIND-210322/286
N/A	09-03-2022	8.8	Windows Event Tracing Remote Code Execution Vulnerability. **CVE ID : CVE-2022-23294**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23294	O-MIC-WIND-210322/287
Improper Privilege Management	09-03-2022	7.8	Windows Installer Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23296**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23296	O-MIC-WIND-210322/288
N/A	09-03-2022	5.5	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23297**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23297	O-MIC-WIND-210322/289
Concurrent Execution using Shared Resource with Improper	09-03-2022	7	Windows NT OS Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23298**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23298	O-MIC-WIND-210322/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')					
Improper Privilege Management	09-03-2022	7.8	Windows PDEV Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23299**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23299	O-MIC-WIND-210322/291
Improper Privilege Management	09-03-2022	7.8	Windows Security Support Provider Interface Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24454**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24454	O-MIC-WIND-210322/292
Improper Privilege Management	09-03-2022	7.8	Windows CD-ROM Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24455**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24455	O-MIC-WIND-210322/293
Improper Privilege Management	09-03-2022	7.8	Windows Fax and Scan Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24459**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24459	O-MIC-WIND-210322/294
Concurrent Execution using Shared Resource with Improper Synchronization	09-03-2022	7	Tablet Windows User Interface Application Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24460**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24460	O-MIC-WIND-210322/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Product: windows_11					
Improper Privilege Management	09-03-2022	7	Xbox Live Auth Manager for Windows Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21967**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21967	O-MIC-WIND-210322/296
N/A	09-03-2022	3.3	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-22010. **CVE ID : CVE-2022-21977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21977	O-MIC-WIND-210322/297
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-23285. **CVE ID : CVE-2022-21990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21990	O-MIC-WIND-210322/298
N/A	09-03-2022	5.5	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-21977. **CVE ID : CVE-2022-22010**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22010	O-MIC-WIND-210322/299
N/A	09-03-2022	6.5	Point-to-Point Tunneling Protocol Denial of	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210322/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service Vulnerability. **CVE ID : CVE-2022-23253**	US/security-guidance/advisory/CVE-2022-23253	
N/A	09-03-2022	5.9	Microsoft Defender for Endpoint Spoofing Vulnerability. **CVE ID : CVE-2022-23278**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23278	O-MIC-WIND-210322/301
N/A	09-03-2022	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23281**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23281	O-MIC-WIND-210322/302
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23287, CVE-2022-24505. **CVE ID : CVE-2022-23283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23283	O-MIC-WIND-210322/303
Improper Privilege Management	09-03-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23284**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23284	O-MIC-WIND-210322/304
Improper Privilege Management	09-03-2022	7	Windows Cloud Files Mini Filter Driver Elevation	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Privilege Vulnerability. **CVE ID : CVE-2022-23286**	ory/CVE-2022-23286	
Improper Privilege Management	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23283, CVE-2022-24505. **CVE ID : CVE-2022-23287**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23287	O-MIC-WIND-210322/306
Improper Privilege Management	09-03-2022	7.8	Windows Inking COM Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23290**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23290	O-MIC-WIND-210322/307
Improper Privilege Management	09-03-2022	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23288. **CVE ID : CVE-2022-23291**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23291	O-MIC-WIND-210322/308
Improper Privilege Management	09-03-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23293**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23293	O-MIC-WIND-210322/309
N/A	09-03-2022	8.8	Windows Event Tracing Remote	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210322/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability. **CVE ID : CVE-2022-23294**	US/security-guidance/advisory/CVE-2022-23294	
Improper Privilege Management	09-03-2022	7.8	Windows Installer Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23296**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23296	O-MIC-WIND-210322/311
N/A	09-03-2022	5.5	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23297**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23297	O-MIC-WIND-210322/312
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows NT OS Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23298**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23298	O-MIC-WIND-210322/313
Improper Privilege Management	09-03-2022	7.8	Windows PDEV Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23299**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23299	O-MIC-WIND-210322/314
Improper Privilege	09-03-2022	7.8	Windows Security Support Provider Interface Elevation of	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210322/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Privilege Vulnerability. **CVE ID : CVE-2022-24454**	guidance/advisory/CVE-2022-24454	
Improper Privilege Management	09-03-2022	7.8	Windows Fax and Scan Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24459**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24459	O-MIC-WIND-210322/316
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Tablet Windows User Interface Application Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24460**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24460	O-MIC-WIND-210322/317
Product: windows_7					
N/A	09-03-2022	5.5	Windows Media Center Update Denial of Service Vulnerability. **CVE ID : CVE-2022-21973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21973	O-MIC-WIND-210322/318
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-23285. **CVE ID : CVE-2022-21990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21990	O-MIC-WIND-210322/319
N/A	09-03-2022	6.5	Point-to-Point Tunneling	https://portal.msrc.microsoft.	O-MIC-WIND-210322/320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-23253**	com/en-US/security-guidance/advisory/CVE-2022-23253	
N/A	09-03-2022	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23281**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23281	O-MIC-WIND-210322/321
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23287, CVE-2022-24505. **CVE ID : CVE-2022-23283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23283	O-MIC-WIND-210322/322
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21990. **CVE ID : CVE-2022-23285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23285	O-MIC-WIND-210322/323
Improper Privilege Management	09-03-2022	7.8	Windows Inking COM Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23290**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23290	O-MIC-WIND-210322/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-03-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23293**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23293	O-MIC-WIND-210322/325
Improper Privilege Management	09-03-2022	7.8	Windows Installer Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23296**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23296	O-MIC-WIND-210322/326
N/A	09-03-2022	5.5	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23297**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23297	O-MIC-WIND-210322/327
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows NT OS Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23298**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23298	O-MIC-WIND-210322/328
Improper Privilege Management	09-03-2022	7.8	Windows PDEV Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23299**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23299	O-MIC-WIND-210322/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-03-2022	7.8	Windows Security Support Provider Interface Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24454**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24454	O-MIC-WIND-210322/330
Improper Privilege Management	09-03-2022	7.8	Windows Fax and Scan Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24459**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24459	O-MIC-WIND-210322/331
Product: windows_8.1					
N/A	09-03-2022	5.5	Windows Media Center Update Denial of Service Vulnerability. **CVE ID : CVE-2022-21973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21973	O-MIC-WIND-210322/332
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	4.7	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-21975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21975	O-MIC-WIND-210322/333
N/A	09-03-2022	3.3	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-22010.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21977	O-MIC-WIND-210322/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21977		
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-23285. **CVE ID : CVE-2022-21990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21990	O-MIC-WIND-210322/335
N/A	09-03-2022	5.5	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-21977. **CVE ID : CVE-2022-22010**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22010	O-MIC-WIND-210322/336
N/A	09-03-2022	6.5	Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-23253**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23253	O-MIC-WIND-210322/337
N/A	09-03-2022	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23281**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23281	O-MIC-WIND-210322/338
Concurrent Execution using Shared Resource with	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			23287, CVE-2022-24505. **CVE ID : CVE-2022-23283**	ory/CVE-2022-23283	
Improper Privilege Management	09-03-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23284**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23284	O-MIC-WIND-210322/340
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21990. **CVE ID : CVE-2022-23285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23285	O-MIC-WIND-210322/341
Improper Privilege Management	09-03-2022	7.8	Windows Inking COM Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23290**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23290	O-MIC-WIND-210322/342
Improper Privilege Management	09-03-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23293**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23293	O-MIC-WIND-210322/343
N/A	09-03-2022	8.8	Windows Event Tracing Remote Code Execution Vulnerability. **CVE ID : CVE-2022-23294**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ory/CVE-2022-23294	
Improper Privilege Management	09-03-2022	7.8	Windows Installer Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23296**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23296	O-MIC-WIND-210322/345
N/A	09-03-2022	5.5	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23297**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23297	O-MIC-WIND-210322/346
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows NT OS Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23298**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23298	O-MIC-WIND-210322/347
Improper Privilege Management	09-03-2022	7.8	Windows PDEV Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23299**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23299	O-MIC-WIND-210322/348
Improper Privilege Management	09-03-2022	7.8	Windows Security Support Provider Interface Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24454	ory/CVE-2022-24454	
Improper Privilege Management	09-03-2022	7.8	Windows CD-ROM Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24455**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24455	O-MIC-WIND-210322/350
Improper Privilege Management	09-03-2022	7.8	Windows Fax and Scan Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24459**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24459	O-MIC-WIND-210322/351
Product: windows_rt_8.1					
N/A	09-03-2022	5.5	Windows Media Center Update Denial of Service Vulnerability. **CVE ID : CVE-2022-21973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21973	O-MIC-WIND-210322/352
N/A	09-03-2022	3.3	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-22010. **CVE ID : CVE-2022-21977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21977	O-MIC-WIND-210322/353
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-23285.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21990	O-MIC-WIND-210322/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21990		
N/A	09-03-2022	5.5	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-21977. **CVE ID : CVE-2022-22010**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22010	O-MIC-WIND-210322/355
N/A	09-03-2022	6.5	Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-23253**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23253	O-MIC-WIND-210322/356
N/A	09-03-2022	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23281**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23281	O-MIC-WIND-210322/357
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23287, CVE-2022-24505. **CVE ID : CVE-2022-23283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23283	O-MIC-WIND-210322/358
Improper Privilege Management	09-03-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210322/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23284	guidance/advisory/CVE-2022-23284	
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21990. **CVE ID : CVE-2022-23285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23285	O-MIC-WIND-210322/360
Improper Privilege Management	09-03-2022	7.8	Windows Inking COM Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23290**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23290	O-MIC-WIND-210322/361
Improper Privilege Management	09-03-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23293**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23293	O-MIC-WIND-210322/362
N/A	09-03-2022	8.8	Windows Event Tracing Remote Code Execution Vulnerability. **CVE ID : CVE-2022-23294**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23294	O-MIC-WIND-210322/363
Improper Privilege Management	09-03-2022	7.8	Windows Installer Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23296**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23296	O-MIC-WIND-210322/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-03-2022	5.5	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23297**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23297	O-MIC-WIND-210322/365
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows NT OS Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23298**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23298	O-MIC-WIND-210322/366
Improper Privilege Management	09-03-2022	7.8	Windows PDEV Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23299**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23299	O-MIC-WIND-210322/367
Improper Privilege Management	09-03-2022	7.8	Windows Security Support Provider Interface Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24454**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24454	O-MIC-WIND-210322/368
Improper Privilege Management	09-03-2022	7.8	Windows CD-ROM Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24455**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24455	O-MIC-WIND-210322/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-03-2022	7.8	Windows Fax and Scan Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24459**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24459	O-MIC-WIND-210322/370
Product: windows_server					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	4.7	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-21975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21975	O-MIC-WIND-210322/371
N/A	09-03-2022	3.3	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-22010. **CVE ID : CVE-2022-21977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21977	O-MIC-WIND-210322/372
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-23285. **CVE ID : CVE-2022-21990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21990	O-MIC-WIND-210322/373
N/A	09-03-2022	5.5	Media Foundation Information Disclosure Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210322/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-21977. **CVE ID : CVE-2022-22010**	guidance/advisory/CVE-2022-22010	
N/A	09-03-2022	6.5	Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-23253**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23253	O-MIC-WIND-210322/375
N/A	09-03-2022	5.9	Microsoft Defender for Endpoint Spoofing Vulnerability. **CVE ID : CVE-2022-23278**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23278	O-MIC-WIND-210322/376
N/A	09-03-2022	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23281**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23281	O-MIC-WIND-210322/377
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23287, CVE-2022-24505. **CVE ID : CVE-2022-23283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23283	O-MIC-WIND-210322/378
Improper Privilege	09-03-2022	7.2	Windows Print Spooler Elevation	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210322/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			of Privilege Vulnerability. **CVE ID : CVE-2022-23284**	US/security-guidance/advisory/CVE-2022-23284	
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21990. **CVE ID : CVE-2022-23285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23285	O-MIC-WIND-210322/380
Improper Privilege Management	09-03-2022	7	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23286**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23286	O-MIC-WIND-210322/381
Improper Privilege Management	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23283, CVE-2022-24505. **CVE ID : CVE-2022-23287**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23287	O-MIC-WIND-210322/382
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows DWM Core Library Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23291. **CVE ID : CVE-2022-23288**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23288	O-MIC-WIND-210322/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-03-2022	7.8	Windows Inking COM Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23290**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23290	O-MIC-WIND-210322/384
Improper Privilege Management	09-03-2022	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23288. **CVE ID : CVE-2022-23291**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23291	O-MIC-WIND-210322/385
Improper Privilege Management	09-03-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23293**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23293	O-MIC-WIND-210322/386
N/A	09-03-2022	8.8	Windows Event Tracing Remote Code Execution Vulnerability. **CVE ID : CVE-2022-23294**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23294	O-MIC-WIND-210322/387
Improper Privilege Management	09-03-2022	7.8	Windows Installer Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23296**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23296	O-MIC-WIND-210322/388
N/A	09-03-2022	5.5	Windows NT Lan Manager Datagram Receiver Driver	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210322/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability. **CVE ID : CVE-2022-23297**	guidance/advisory/CVE-2022-23297	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows NT OS Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23298**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23298	O-MIC-WIND-210322/390
Improper Privilege Management	09-03-2022	7.8	Windows PDEV Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23299**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23299	O-MIC-WIND-210322/391
Improper Privilege Management	09-03-2022	7.8	Windows Security Support Provider Interface Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24454**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24454	O-MIC-WIND-210322/392
Improper Privilege Management	09-03-2022	7.8	Windows Fax and Scan Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24459**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24459	O-MIC-WIND-210322/393
Concurrent Execution using	09-03-2022	7	Tablet Windows User Interface Application	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210322/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24460**	US/security-guidance/advisory/CVE-2022-24460	
Product: windows_server_2008					
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-23285. **CVE ID : CVE-2022-21990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21990	O-MIC-WIND-210322/395
N/A	09-03-2022	6.5	Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-23253**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23253	O-MIC-WIND-210322/396
N/A	09-03-2022	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23281**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23281	O-MIC-WIND-210322/397
Concurrent Execution using Shared Resource with Improper Synchroniz	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23287, CVE-2022-24505.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23283	O-MIC-WIND-210322/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			**CVE ID : CVE-2022-23283**		
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21990. **CVE ID : CVE-2022-23285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23285	O-MIC-WIND-210322/399
Improper Privilege Management	09-03-2022	7.8	Windows Inking COM Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23290**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23290	O-MIC-WIND-210322/400
Improper Privilege Management	09-03-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23293**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23293	O-MIC-WIND-210322/401
Improper Privilege Management	09-03-2022	7.8	Windows Installer Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23296**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23296	O-MIC-WIND-210322/402
N/A	09-03-2022	5.5	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23297	O-MIC-WIND-210322/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23297		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows NT OS Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23298**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23298	O-MIC-WIND-210322/404
Improper Privilege Management	09-03-2022	7.8	Windows PDEV Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23299**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23299	O-MIC-WIND-210322/405
Improper Privilege Management	09-03-2022	7.8	Windows Security Support Provider Interface Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24454**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24454	O-MIC-WIND-210322/406
Improper Privilege Management	09-03-2022	7.8	Windows Fax and Scan Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24459**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24459	O-MIC-WIND-210322/407
Product: windows_server_2012					
N/A	09-03-2022	5.5	Windows Media Center Update Denial of Service Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21973	ory/CVE-2022-21973	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	4.7	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-21975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21975	O-MIC-WIND-210322/409
N/A	09-03-2022	3.3	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-22010. **CVE ID : CVE-2022-21977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21977	O-MIC-WIND-210322/410
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-23285. **CVE ID : CVE-2022-21990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21990	O-MIC-WIND-210322/411
N/A	09-03-2022	5.5	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-21977. **CVE ID : CVE-2022-22010**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22010	O-MIC-WIND-210322/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-03-2022	6.5	Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-23253**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23253	O-MIC-WIND-210322/413
N/A	09-03-2022	5.9	Microsoft Defender for Endpoint Spoofing Vulnerability. **CVE ID : CVE-2022-23278**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23278	O-MIC-WIND-210322/414
N/A	09-03-2022	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23281**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23281	O-MIC-WIND-210322/415
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23287, CVE-2022-24505. **CVE ID : CVE-2022-23283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23283	O-MIC-WIND-210322/416
Improper Privilege Management	09-03-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23284**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23284	O-MIC-WIND-210322/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21990. **CVE ID : CVE-2022-23285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23285	O-MIC-WIND-210322/418
Improper Privilege Management	09-03-2022	7.8	Windows Inking COM Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23290**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23290	O-MIC-WIND-210322/419
Improper Privilege Management	09-03-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23293**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23293	O-MIC-WIND-210322/420
N/A	09-03-2022	8.8	Windows Event Tracing Remote Code Execution Vulnerability. **CVE ID : CVE-2022-23294**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23294	O-MIC-WIND-210322/421
Improper Privilege Management	09-03-2022	7.8	Windows Installer Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23296**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23296	O-MIC-WIND-210322/422
N/A	09-03-2022	5.5	Windows NT Lan Manager Datagram Receiver Driver Information	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability. **CVE ID : CVE-2022-23297**	ory/CVE-2022-23297	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows NT OS Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23298**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23298	O-MIC-WIND-210322/424
Improper Privilege Management	09-03-2022	7.8	Windows PDEV Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23299**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23299	O-MIC-WIND-210322/425
Improper Privilege Management	09-03-2022	7.8	Windows Security Support Provider Interface Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24454**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24454	O-MIC-WIND-210322/426
Improper Privilege Management	09-03-2022	7.8	Windows CD-ROM Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24455**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24455	O-MIC-WIND-210322/427
Improper Privilege Management	09-03-2022	7.8	Windows Fax and Scan Service Elevation of	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-24459**	ory/CVE-2022-24459	
Product: windows_server_2016					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	4.7	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-21975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21975	O-MIC-WIND-210322/429
N/A	09-03-2022	3.3	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-22010. **CVE ID : CVE-2022-21977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21977	O-MIC-WIND-210322/430
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-23285. **CVE ID : CVE-2022-21990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21990	O-MIC-WIND-210322/431
N/A	09-03-2022	5.5	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-21977.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22010	O-MIC-WIND-210322/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22010		
N/A	09-03-2022	6.5	Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-23253**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23253	O-MIC-WIND-210322/433
N/A	09-03-2022	5.9	Microsoft Defender for Endpoint Spoofing Vulnerability. **CVE ID : CVE-2022-23278**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23278	O-MIC-WIND-210322/434
N/A	09-03-2022	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23281**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23281	O-MIC-WIND-210322/435
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23287, CVE-2022-24505. **CVE ID : CVE-2022-23283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23283	O-MIC-WIND-210322/436
Improper Privilege Management	09-03-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23284**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ory/CVE-2022-23284	
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21990. **CVE ID : CVE-2022-23285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23285	O-MIC-WIND-210322/438
Improper Privilege Management	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23283, CVE-2022-24505. **CVE ID : CVE-2022-23287**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23287	O-MIC-WIND-210322/439
Improper Privilege Management	09-03-2022	7.8	Windows Inking COM Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23290**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23290	O-MIC-WIND-210322/440
Improper Privilege Management	09-03-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23293**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23293	O-MIC-WIND-210322/441
N/A	09-03-2022	8.8	Windows Event Tracing Remote Code Execution Vulnerability. **CVE ID : CVE-2022-23294**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ory/CVE-2022-23294	
Improper Privilege Management	09-03-2022	7.8	Windows Installer Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23296**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23296	O-MIC-WIND-210322/443
N/A	09-03-2022	5.5	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23297**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23297	O-MIC-WIND-210322/444
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows NT OS Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23298**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23298	O-MIC-WIND-210322/445
Improper Privilege Management	09-03-2022	7.8	Windows PDEV Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23299**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23299	O-MIC-WIND-210322/446
Improper Privilege Management	09-03-2022	7.8	Windows Security Support Provider Interface Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24454	ory/CVE-2022-24454	
Improper Privilege Management	09-03-2022	7.8	Windows CD-ROM Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24455**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24455	O-MIC-WIND-210322/448
Improper Privilege Management	09-03-2022	7.8	Windows Fax and Scan Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24459**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24459	O-MIC-WIND-210322/449
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Tablet Windows User Interface Application Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24460**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24460	O-MIC-WIND-210322/450
Product: windows_server_2019					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	4.7	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-21975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21975	O-MIC-WIND-210322/451
N/A	09-03-2022	3.3	Media Foundation Information Disclosure	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210322/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-22010. **CVE ID : CVE-2022-21977**	US/security-guidance/advisory/CVE-2022-21977	
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-23285. **CVE ID : CVE-2022-21990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21990	O-MIC-WIND-210322/453
N/A	09-03-2022	5.5	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-21977. **CVE ID : CVE-2022-22010**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22010	O-MIC-WIND-210322/454
N/A	09-03-2022	6.5	Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-23253**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23253	O-MIC-WIND-210322/455
N/A	09-03-2022	5.9	Microsoft Defender for Endpoint Spoofing Vulnerability. **CVE ID : CVE-2022-23278**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23278	O-MIC-WIND-210322/456
N/A	09-03-2022	5.5	Windows Common Log File System Driver	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210322/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability. **CVE ID : CVE-2022-23281**	US/security-guidance/advisory/CVE-2022-23281	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows ALPC Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23287, CVE-2022-24505. **CVE ID : CVE-2022-23283**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23283	O-MIC-WIND-210322/458
Improper Privilege Management	09-03-2022	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23284**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23284	O-MIC-WIND-210322/459
N/A	09-03-2022	8.8	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21990. **CVE ID : CVE-2022-23285**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23285	O-MIC-WIND-210322/460
Improper Privilege Management	09-03-2022	7	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23286**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23286	O-MIC-WIND-210322/461
Improper Privilege	09-03-2022	7	Windows ALPC Elevation of	https://portal.msrc.microsoft.	O-MIC-WIND-210322/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Privilege Vulnerability. This CVE ID is unique from CVE-2022-23283, CVE-2022-24505. **CVE ID : CVE-2022-23287**	com/en-US/security-guidance/advisory/CVE-2022-23287	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows DWM Core Library Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23291. **CVE ID : CVE-2022-23288**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23288	O-MIC-WIND-210322/463
Improper Privilege Management	09-03-2022	7.8	Windows Inking COM Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23290**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23290	O-MIC-WIND-210322/464
Improper Privilege Management	09-03-2022	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23288. **CVE ID : CVE-2022-23291**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23291	O-MIC-WIND-210322/465
Improper Privilege Management	09-03-2022	7.8	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23293	ory/CVE-2022-23293	
N/A	09-03-2022	8.8	Windows Event Tracing Remote Code Execution Vulnerability. **CVE ID : CVE-2022-23294**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23294	O-MIC-WIND-210322/467
Improper Privilege Management	09-03-2022	7.8	Windows Installer Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23296**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23296	O-MIC-WIND-210322/468
N/A	09-03-2022	5.5	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-23297**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23297	O-MIC-WIND-210322/469
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Windows NT OS Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23298**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23298	O-MIC-WIND-210322/470
Improper Privilege Management	09-03-2022	7.8	Windows PDEV Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23299	ory/CVE-2022-23299	
Improper Privilege Management	09-03-2022	7.8	Windows Security Support Provider Interface Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24454**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24454	O-MIC-WIND-210322/472
Improper Privilege Management	09-03-2022	7.8	Windows CD-ROM Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24455**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24455	O-MIC-WIND-210322/473
Improper Privilege Management	09-03-2022	7.8	Windows Fax and Scan Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24459**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24459	O-MIC-WIND-210322/474
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-03-2022	7	Tablet Windows User Interface Application Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-24460**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24460	O-MIC-WIND-210322/475
Product: windows_server_2022					
N/A	09-03-2022	3.3	Media Foundation Information Disclosure Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-210322/476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-22010. **CVE ID : CVE-2022-21977**	ory/CVE-2022-21977	
Vendor: Paloaltonetworks					
Product: pan-os					
Use of Password Hash With Insufficient Computational Effort	09-03-2022	4.4	Usage of a weak cryptographic algorithm in Palo Alto Networks PAN-OS software where the password hashes of administrator and local user accounts are not created with a sufficient level of computational effort, which allows for password cracking attacks on accounts in normal (non-FIPS-CC) operational mode. An attacker must have access to the account password hashes to take advantage of this weakness and can acquire those hashes if they are able to gain access to the PAN-OS software configuration. Fixed versions of PAN-OS software use a secure cryptographic algorithm for	https://security.paloaltonetworks.com/CVE-2022-0022	O-PAL-PAN--210322/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account password hashes. This issue does not impact Prisma Access firewalls. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.21; All versions of PAN-OS 9.0; PAN-OS 9.1 versions earlier than PAN-OS 9.1.11; PAN-OS 10.0 versions earlier than PAN-OS 10.0.7. **CVE ID : CVE-2022-0022**		
Vendor: Redhat					
Product: enterprise_linux					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-03-2022	7.5	A flaw was found in the way HAProxy processed HTTP responses containing the "Set-Cookie2" header. This flaw could allow an attacker to send crafted HTTP response packets which lead to an infinite loop, eventually resulting in a denial of service condition. The highest threat from this	https://github.com/haproxy/haproxy/commit/bfb15ab34ead85f64cd6da0e9fb418c9cd14cee8	O-RED-ENTE-210322/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is availability. **CVE ID : CVE-2022-0711**		
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/479
Product: enterprise_linux_eus					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**		
Product: enterprise_linux_for_ibm_z_systems					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system.	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0847		
Product: enterprise_linux_for_ibm_z_systems_eus					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/482
Product: enterprise_linux_for_power_little_endian					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**		
Product: enterprise_linux_for_power_little_endian_eus					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system.	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0847		
Product: enterprise_linux_for_real_time					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/485
Product: enterprise_linux_for_real_time_for_nfv					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**		
Product: enterprise_linux_for_real_time_for_nfv_tus					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system.	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0847		
Product: enterprise_linux_for_real_time_tus					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/488
Product: enterprise_linux_server_aus					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**		
Product: enterprise_linux_server_for_power_little_endian_update_services_for_sap_solutions					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system.	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0847		
Product: enterprise_linux_server_tus					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/491
Product: enterprise_linux_server_update_services_for_sap_solutions					
Improper Initialization	10-03-2022	7.8	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe	https://bugzilla.redhat.com/show_bug.cgi?id=2060795	O-RED-ENTE-210322/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system. **CVE ID : CVE-2022-0847**		
Vendor: Siemens					
Product: sinumerik_mc_firmware					
Improper Privilege Management	08-03-2022	7.8	A vulnerability has been identified in SINUMERIK MC (All versions < V1.15 SP1), SINUMERIK ONE (All versions < V6.15 SP1). The sc SUID binary on affected devices provides several commands that are used to execute system commands or modify system files. A specific set of operations using sc could allow local attackers to escalate their privileges to root.	https://cert-portal.siemens.com/productcert/pdf/ssa-337210.pdf	O-SIE-SINU-210322/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24408		
Product: sinumerik_one_firmware					
Improper Privilege Management	08-03-2022	7.8	A vulnerability has been identified in SINUMERIK MC (All versions < V1.15 SP1), SINUMERIK ONE (All versions < V6.15 SP1). The sc SUID binary on affected devices provides several commands that are used to execute system commands or modify system files. A specific set of operations using sc could allow local attackers to escalate their privileges to root. **CVE ID : CVE-2022-24408**	https://cert-portal.siemens.com/productcert/pdf/ssa-337210.pdf	O-SIE-SINU-210322/494
Vendor: Tenda					
Product: ax1806_firmware					
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial	N/A	O-TEN-AX18-210322/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service (DoS) via the ddnsUser parameter. **CVE ID : CVE-2022-25546**		
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the time parameter. **CVE ID : CVE-2022-25547**	N/A	O-TEN-AX18-210322/496
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the serverName parameter. **CVE ID : CVE-2022-25548**	N/A	O-TEN-AX18-210322/497
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function	N/A	O-TEN-AX18-210322/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsEn parameter. **CVE ID : CVE-2022-25549**		
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the deviceName parameter. **CVE ID : CVE-2022-25550**	N/A	O-TEN-AX18-210322/499
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsDomain parameter.	N/A	O-TEN-AX18-210322/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25551		
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function form_fast_setting_wifi_set. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ssid parameter. **CVE ID : CVE-2022-25552**	N/A	O-TEN-AX18-210322/501
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsPwd parameter. **CVE ID : CVE-2022-25553**	N/A	O-TEN-AX18-210322/502
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function saveParentControlInfo. This	N/A	O-TEN-AX18-210322/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows attackers to cause a Denial of Service (DoS) via the deviceId parameter. **CVE ID : CVE-2022-25554**		
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ntpServer parameter. **CVE ID : CVE-2022-25555**	N/A	O-TEN-AX18-210322/504
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a heap overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the urls parameter. **CVE ID : CVE-2022-25557**	N/A	O-TEN-AX18-210322/505
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to	N/A	O-TEN-AX18-210322/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a stack overflow in the function formSetProvince. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ProvinceCode parameter. **CVE ID : CVE-2022-25558**		
Out-of-bounds Write	10-03-2022	7.5	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the time parameter. **CVE ID : CVE-2022-25566**	N/A	O-TEN-AX18-210322/507