National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

01 – 15 Mar 2024 Vol. 11 No. 05

Table of Content

Vendor	Product	Page Number
Application		
Apple	safari	1
cisa	icsnpp-ethercat	1
Fortinet	forticlient_endpoint_management_server	3
	forticlient_enterprise_management_server	5
	fortimanager	6
	fortiproxy	9
Hikvision	hikcentral_professional	15
Jetbrains	teamcity	15
Qnap	myqnapcloud	16
Vmware	cloud_director	16
Hardware		
Tp-link	tl-sg2210p	17
Operating System		
Apple	ipad_os	17
	iphone_os	20
	macos	24
	tvos	35
	visionos	37
	watchos	38
Fortinet	fortios	39
Qnap	qts	48
	qutscloud	54
	quts_hero	56
Tp-link	tl-sg2210p_firmware	61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: Apple					
Product: safari					
Affected Version(s): * Up to (excluding) 17.4					
N/A	08-Mar-2024	4.3	This issue was addressed through improved state management. This issue is fixed in Safari 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4. Private Browsing tabs may be accessed without authentication. **CVE ID : CVE-2024-23273**	https://support.apple.com/en-us/HT214081 , https://support.apple.com/en-us/HT214084 , https://support.apple.com/en-us/HT214089	A-APP-SAFA-200324/1
Vendor: cisa					
Product: icsnpp-ethercat					
Affected Version(s): * Up to (including) d78dda6					
Out-of-bounds Write	01-Mar-2024	9.8	Industrial Control Systems Network Protocol Parsers (ICSNPP) - Ethercat Zeek Plugin versions d78dda6 and prior are vulnerable to out-of-bounds write while analyzing specific Ethercat datagrams. This could allow an	https://www.cisa.gov/news-events/ics-advisories/icsa-24-051-02	A-CIS-ICSN-200324/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause arbitrary code execution. **CVE ID : CVE-2023-7243**		
Out-of-bounds Write	01-Mar-2024	9.8	Industrial Control Systems Network Protocol Parsers (ICSNPP) - Ethercat Zeek Plugin versions d78dda6 and prior are vulnerable to out-of-bounds write in their primary analyses function for Ethercat communication packets. This could allow an attacker to cause arbitrary code execution. **CVE ID : CVE-2023-7244**	https://www.cisa.gov/news-events/ics-advisories/icsa-24-051-02	A-CIS-ICSN-200324/3
Out-of-bounds Read	01-Mar-2024	8.2	Industrial Control Systems Network Protocol Parsers (ICSNPP) - Ethercat Zeek Plugin versions d78dda6 and prior are vulnerable to out-of-bounds read during the process of analyzing a specific Ethercat packet. This could allow an attacker to crash	https://www.cisa.gov/news-events/ics-advisories/icsa-24-051-02	A-CIS-ICSN-200324/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Zeek process and leak some information in memory. **CVE ID : CVE-2023-7242**		
Vendor: Fortinet					
Product: forticlient_endpoint_management_server					
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.8					
Improper Neutralization of Formula Elements in a CSV File	12-Mar-2024	8.8	A improper neutralization of formula elements in a csv file in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.10, 6.4.0 through 6.4.9, 6.2.0 through 6.2.9, 6.0.0 through 6.0.8 allows attacker to execute unauthorized code or commands via specially crafted packets. **CVE ID : CVE-2023-47534**	https://fortiguard.com/psirt/FG-IR-23-390	A-FOR-FORT-200324/5
Affected Version(s): From (including) 6.2.0 Up to (including) 6.2.9					
Improper Neutralization of Formula Elements in a CSV File	12-Mar-2024	8.8	A improper neutralization of formula elements in a csv file in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.10, 6.4.0 through 6.4.9, 6.2.0 through 6.2.9,	https://fortiguard.com/psirt/FG-IR-23-390	A-FOR-FORT-200324/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.0.0 through 6.0.8 allows attacker to execute unauthorized code or commands via specially crafted packets. **CVE ID : CVE-2023-47534**		
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.9					
Improper Neutralization of Formula Elements in a CSV File	12-Mar-2024	8.8	A improper neutralization of formula elements in a csv file in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.10, 6.4.0 through 6.4.9, 6.2.0 through 6.2.9, 6.0.0 through 6.0.8 allows attacker to execute unauthorized code or commands via specially crafted packets. **CVE ID : CVE-2023-47534**	https://fortiguard.com/psirt/FG-IR-23-390	A-FOR-FORT-200324/7
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.10					
Improper Neutralization of Formula Elements in a CSV File	12-Mar-2024	8.8	A improper neutralization of formula elements in a csv file in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.10, 6.4.0 through 6.4.9, 6.2.0 through 6.2.9,	https://fortiguard.com/psirt/FG-IR-23-390	A-FOR-FORT-200324/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.0.0 through 6.0.8 allows attacker to execute unauthorized code or commands via specially crafted packets. **CVE ID : CVE-2023-47534**		
Affected Version(s): From (including) 7.2.0 Up to (including) 7.2.2					
Improper Neutralization of Formula Elements in a CSV File	12-Mar-2024	8.8	A improper neutralization of formula elements in a csv file in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.10, 6.4.0 through 6.4.9, 6.2.0 through 6.2.9, 6.0.0 through 6.0.8 allows attacker to execute unauthorized code or commands via specially crafted packets. **CVE ID : CVE-2023-47534**	https://fortiguard.com/psirt/FG-IR-23-390	A-FOR-FORT-200324/9
Product: forticlient_enterprise_management_server					
Affected Version(s): From (including) 7.2.0 Up to (including) 7.2.2					
Improper Neutralization of Special Elements used in an SQL Command	12-Mar-2024	9.8	A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiClientEMS version 7.2.0 through 7.2.2,	https://fortiguard.com/psirt/FG-IR-23-430	A-FOR-FORT-200324/10

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')			FortiClientEMS 7.0.1 through 7.0.10 allows attacker to execute unauthorized code or commands via specially crafted packets. **CVE ID : CVE-2023-48788**		
Affected Version(s): From (including) 7.0.1 Up to (including) 7.0.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Mar-2024	9.8	A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, FortiClientEMS 7.0.1 through 7.0.10 allows attacker to execute unauthorized code or commands via specially crafted packets. **CVE ID : CVE-2023-48788**	https://fortiguard.com/psirt/FG-IR-23-430	A-FOR-FORT-200324/11
Product: fortimanager					
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.10					
Improper Access Control	12-Mar-2024	9.8	A improper access control in Fortinet FortiManager version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.10, version 6.4.0	https://fortiguard.com/psirt/FG-IR-23-103	A-FOR-FORT-200324/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 6.4.13, 6.2 all versions allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-36554**		
Affected Version(s): 7.4.0					
Improper Access Control	12-Mar-2024	9.8	A improper access control in Fortinet FortiManager version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.10, version 6.4.0 through 6.4.13, 6.2 all versions allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-36554**	https://fortiguard.com/psirt/FG-IR-23-103	A-FOR-FORT-200324/13
Affected Version(s): From (including) 6.2.0 Up to (including) 6.2.12					
Improper Access Control	12-Mar-2024	9.8	A improper access control in Fortinet FortiManager version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.10, version 6.4.0 through 6.4.13, 6.2 all versions allows attacker to execute unauthorized code	https://fortiguard.com/psirt/FG-IR-23-103	A-FOR-FORT-200324/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-36554**		
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.13					
Improper Access Control	12-Mar-2024	9.8	A improper access control in Fortinet FortiManager version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.10, version 6.4.0 through 6.4.13, 6.2 all versions allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-36554**	https://fortiguard.com/psirt/FG-IR-23-103	A-FOR-FORT-200324/15
Affected Version(s): From (including) 7.2.0 Up to (including) 7.2.3					
Improper Access Control	12-Mar-2024	9.8	A improper access control in Fortinet FortiManager version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.10, version 6.4.0 through 6.4.13, 6.2 all versions allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.	https://fortiguard.com/psirt/FG-IR-23-103	A-FOR-FORT-200324/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36554		
Product: fortiproxy					
Affected Version(s): 7.4.0					
Out-of-bounds Write	12-Mar-2024	9.8	A out-of-bounds write in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42789**	https://fortiguard.com/psirt/FG-IR-23-328	A-FOR-FORT-200324/17
Stack-based Buffer Overflow	12-Mar-2024	8.1	A stack-based buffer overflow in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute	https://fortiguard.com/psirt/FG-IR-23-327	A-FOR-FORT-200324/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42790**		
Affected Version(s): From (including) 2.0.0 Up to (including) 2.0.13					
Out-of-bounds Write	12-Mar-2024	9.8	A out-of-bounds write in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42789**	https://fortiguard.com/psirt/FG-IR-23-328	A-FOR-FORT-200324/19
Stack-based Buffer Overflow	12-Mar-2024	8.1	A stack-based buffer overflow in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0	https://fortiguard.com/psirt/FG-IR-23-327	A-FOR-FORT-200324/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42790**		
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.12					
Out-of-bounds Write	12-Mar-2024	9.8	A out-of-bounds write in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42789**	https://fortiguard.com/psirt/FG-IR-23-328	A-FOR-FORT-200324/21
Stack-based Buffer Overflow	12-Mar-2024	8.1	A stack-based buffer overflow in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy	https://fortiguard.com/psirt/FG-IR-23-327	A-FOR-FORT-200324/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42790**		
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.14					
Authorization Bypass Through User-Controlled Key	12-Mar-2024	4.3	An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiOS version 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.1 through 7.0.13, 6.4.7 through 6.4.14, and FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 SSL-VPN may allow an authenticated attacker to gain access to another user's bookmark via URL manipulation. **CVE ID : CVE-2024-23112**	https://fortiguard.com/psirt/FG-IR-24-013	A-FOR-FORT-200324/23
Affected Version(s): From (including) 7.2.0 Up to (including) 7.2.6					
Out-of-bounds Write	12-Mar-2024	9.8	A out-of-bounds write in Fortinet FortiOS 7.4.0	https://fortiguard.com/psir	A-FOR-FORT-200324/24

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
			through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42789**	t/FG-IR-23-328	
Stack-based Buffer Overflow	12-Mar-2024	8.1	A stack-based buffer overflow in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42790**	https://fortiguard.com/psirt/FG-IR-23-327	A-FOR-FORT-200324/25
Affected Version(s): From (including) 7.2.0 Up to (including) 7.2.8					

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
Authorization Bypass Through User-Controlled Key	12-Mar-2024	4.3	An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiOS version 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.1 through 7.0.13, 6.4.7 through 6.4.14, and FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 SSL-VPN may allow an authenticated attacker to gain access to another user's bookmark via URL manipulation. **CVE ID : CVE-2024-23112**	https://fortiguard.com/psirt/FG-IR-24-013	A-FOR-FORT-200324/26
Affected Version(s): From (including) 7.4.0 Up to (including) 7.4.2					
Authorization Bypass Through User-Controlled Key	12-Mar-2024	4.3	An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiOS version 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.1 through 7.0.13, 6.4.7 through 6.4.14, and FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 SSL-VPN may allow an	https://fortiguard.com/psirt/FG-IR-24-013	A-FOR-FORT-200324/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker to gain access to another user’s bookmark via URL manipulation. **CVE ID : CVE-2024-23112**		
Vendor: Hikvision					
Product: hikcentral_professional					
Affected Version(s): * Up to (including) 2.5.1					
N/A	02-Mar-2024	7.5	Due to insufficient server-side validation, a successful exploit of this vulnerability could allow an attacker to gain access to certain URLs that the attacker should not have access to. **CVE ID : CVE-2024-25063**	https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-vulnerabilities-in-hikcentral-professional/	A-HIK-HIKC-200324/28
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.5.1					
N/A	02-Mar-2024	4.3	Due to insufficient server-side validation, an attacker with login privileges could access certain resources that the attacker should not have access to by changing parameter values. **CVE ID : CVE-2024-25064**	https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-vulnerabilities-in-hikcentral-professional/	A-HIK-HIKC-200324/29
Vendor: Jetbrains					
Product: teamcity					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2023.11.4					
N/A	04-Mar-2024	9.8	In JetBrains TeamCity before 2023.11.4 authentication bypass allowing to perform admin actions was possible **CVE ID : CVE-2024-27198**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-200324/30
Vendor: Qnap					
Product: myqnapcloud					
Affected Version(s): * Up to (excluding) 1.0.52					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Mar-2024	4.7	A SQL injection vulnerability has been reported to affect myQNAPcloud. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: myQNAPcloud 1.0.52 (2023/11/24) and later QTS 4.5.4.2627 build 20231225 and later **CVE ID : CVE-2024-21901**	https://www.qnap.com/en/security-advisory/qsa-24-09	A-QNA-MYQN-200324/31
Vendor: Vmware					
Product: cloud_director					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 10.4.0 Up to (excluding) 10.5.1.1					
N/A	07-Mar-2024	4.3	VMware Cloud Director contains a partial information disclosure vulnerability. A malicious actor can potentially gather information about organization names based on the behavior of the instance. **CVE ID : CVE-2024-22256**	https://www.vmware.com/security/advisories/VMSA-2024-0007.html	A-VMW-CLOU-200324/32
Hardware					
Vendor: Tp-link					
Product: tl-sg2210p					
Affected Version(s): -					
N/A	06-Mar-2024	8.8	TP-Link JetStream Smart Switch TL-SG2210P 5.0 Build 20211201 allows attackers to escalate privileges via modification of the 'tid' and 'usrlvl' values in GET requests. **CVE ID : CVE-2023-43318**	N/A	H-TP--TL-S-200324/33
Operating System					
Vendor: Apple					
Product: ipad_os					
Affected Version(s): * Up to (excluding) 16.7.6					
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved	https://support.apple.com/en-us/HT214081	O-APP-IPAD-200324/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23225**	, https://support.apple.com/en-us/HT214082 , https://support.apple.com/kb/HT214083 , https://support.apple.com/kb/HT214084 , https://support.apple.com/kb/HT214085 , https://support.apple.com/kb/HT214086	
Affected Version(s): * Up to (excluding) 17.4					
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23296**	https://support.apple.com/en-us/HT214081 , https://support.apple.com/kb/HT214084 , https://support.apple.com/kb/HT214086 , https://support.apple.com/kb/HT214087 , https://support.apple.com/kb/HT214088	O-APP-IPAD-200324/35

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	08-Mar-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.7.4, macOS Ventura 13.6.5, macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, tvOS 17.4. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23270**	https://support.apple.com/en-us/HT214081, https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085, https://support.apple.com/en-us/HT214086	O-APP-IPAD-200324/36
N/A	08-Mar-2024	4.3	This issue was addressed through improved state management. This issue is fixed in Safari 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4. Private Browsing tabs may be accessed without authentication. **CVE ID : CVE-2024-23273**	https://support.apple.com/en-us/HT214081, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214089	O-APP-IPAD-200324/37
Affected Version(s): From (excluding) 17.0 Up to (excluding) 17.4					
N/A	08-Mar-2024	5.9	The issue was addressed with improved checks.	https://support.apple.com/en-	O-APP-IPAD-200324/38

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 macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4. An attacker in a privileged network position may be able to inject keystrokes by spoofing a keyboard. **CVE ID : CVE-2024-23277**	us/HT214081 , https://support.apple.com/en-us/HT214084	
Affected Version(s): From (including) 17.0 Up to (excluding) 17.4					
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23225**	https://support.apple.com/en-us/HT214081 , https://support.apple.com/en-us/HT214082 , https://support.apple.com/kb/HT214083 , https://support.apple.com/kb/HT214084 , https://support.apple.com/kb/HT214085 , https://support.apple.com/kb/HT214086	O-APP-IPAD-200324/39
Product: iphone_os					
Affected Version(s): * Up to (excluding) 16.7.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23225**	https://support.apple.com/en-us/HT214081 , https://support.apple.com/en-us/HT214082 , https://support.apple.com/kb/HT214083 , https://support.apple.com/kb/HT214084 , https://support.apple.com/kb/HT214085 , https://support.apple.com/kb/HT214086	O-APP-IPHO-200324/40
Affected Version(s): * Up to (excluding) 17.4					
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may	https://support.apple.com/en-us/HT214081 , https://support.apple.com/kb/HT214084 , https://support.apple.com/kb/HT214086 , https://support.apple.com/kb/HT214087 ,	O-APP-IPHO-200324/41

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have been exploited. **CVE ID : CVE-2024-23296**	https://support.apple.com/kb/HT214088	
N/A	08-Mar-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.7.4, macOS Ventura 13.6.5, macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, tvOS 17.4. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23270**	https://support.apple.com/en-us/HT214081, https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085, https://support.apple.com/en-us/HT214086	O-APP-IPHO-200324/42
N/A	08-Mar-2024	4.3	This issue was addressed through improved state management. This issue is fixed in Safari 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4. Private Browsing tabs may be accessed without authentication.	https://support.apple.com/en-us/HT214081, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214089	O-APP-IPHO-200324/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23273		
Affected Version(s): From (including) 17.0 Up to (excluding) 17.4					
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23225**	https://support.apple.com/en-us/HT214081 , https://support.apple.com/en-us/HT214082 , https://support.apple.com/kb/HT214083 , https://support.apple.com/kb/HT214084 , https://support.apple.com/kb/HT214085 , https://support.apple.com/kb/HT214086	O-APP-IPHO-200324/44
N/A	08-Mar-2024	5.9	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4. An attacker in a privileged network position may be able to inject keystrokes by spoofing a keyboard.	https://support.apple.com/en-us/HT214081 , https://support.apple.com/en-us/HT214084	O-APP-IPHO-200324/45

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-2024-23277		
Product: macos					
Affected Version(s): From (including) 12.0 Up to (excluding) 12.7.4					
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23225**	https://support.apple.com/en-us/HT214081, https://support.apple.com/en-us/HT214082, https://support.apple.com/kb/HT214083, https://support.apple.com/kb/HT214084, https://support.apple.com/kb/HT214085, https://support.apple.com/kb/HT214086	O-APP-MACO-200324/46
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.7.4					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	08-Mar-2024	7.8	An injection issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges.	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/	O-APP-MACO-200324/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			**CVE ID : CVE-2024-23268**	en-us/HT214085	
N/A	08-Mar-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.7.4, macOS Ventura 13.6.5, macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, tvOS 17.4. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23270**	https://support.apple.com/en-us/HT214081 , https://support.apple.com/en-us/HT214083 , https://support.apple.com/en-us/HT214084 , https://support.apple.com/en-us/HT214085 , https://support.apple.com/en-us/HT214086	O-APP-MACO-200324/48
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Mar-2024	7.8	An injection issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges. **CVE ID : CVE-2024-23274**	https://support.apple.com/en-us/HT214083 , https://support.apple.com/en-us/HT214084 , https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/49
N/A	08-Mar-2024	7.8	A logic issue was addressed with improved checks.	https://support.apple.com/en-	O-APP-MACO-200324/50

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 macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges. **CVE ID : CVE-2024-23276**	us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085	
N/A	08-Mar-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2024-23266**	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/51
N/A	08-Mar-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to bypass certain Privacy preferences. **CVE ID : CVE-2024-23267**	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/52
N/A	08-Mar-2024	5.5	A logic issue was addressed with improved checks.	https://support.apple.com/en-	O-APP-MACO-200324/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. A user may gain access to protected parts of the file system. **CVE ID : CVE-2024-23272**	us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Mar-2024	4.7	A race condition was addressed with additional validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to access protected user data. **CVE ID : CVE-2024-23275**	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/54
Affected Version(s): From (including) 13.0 Up to (excluding) 13.6.5					
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple	https://support.apple.com/en-us/HT214081, https://support.apple.com/en-us/HT214082, https://support.apple.com/kb/HT214083, https://support.apple.com/	O-APP-MACO-200324/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23225**	kb/HT214084 , https://support.apple.com/kb/HT214085 , https://support.apple.com/kb/HT214086	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Mar-2024	7.8	An injection issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges. **CVE ID : CVE-2024-23268**	https://support.apple.com/en-us/HT214083 , https://support.apple.com/en-us/HT214084 , https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/56
N/A	08-Mar-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.7.4, macOS Ventura 13.6.5, macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, tvOS 17.4. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23270**	https://support.apple.com/en-us/HT214081 , https://support.apple.com/en-us/HT214083 , https://support.apple.com/en-us/HT214084 , https://support.apple.com/en-us/HT214085 ,	O-APP-MACO-200324/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT214086	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Mar-2024	7.8	An injection issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges. **CVE ID : CVE-2024-23274**	https://support.apple.com/en-us/HT214083 , https://support.apple.com/en-us/HT214084 , https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/58
N/A	08-Mar-2024	7.8	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges. **CVE ID : CVE-2024-23276**	https://support.apple.com/en-us/HT214083 , https://support.apple.com/en-us/HT214084 , https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/59
N/A	08-Mar-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to modify	https://support.apple.com/en-us/HT214083 , https://support.apple.com/en-us/HT214084 , https://suppo	O-APP-MACO-200324/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected parts of the file system. **CVE ID : CVE-2024-23266**	rt.apple.com/en-us/HT214085	
N/A	08-Mar-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to bypass certain Privacy preferences. **CVE ID : CVE-2024-23267**	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/61
N/A	08-Mar-2024	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. A user may gain access to protected parts of the file system. **CVE ID : CVE-2024-23272**	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/62
Concurrent Execution using Shared Resource with Improper Synchronization	08-Mar-2024	4.7	A race condition was addressed with additional validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084,	O-APP-MACO-200324/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			be able to access protected user data. **CVE ID : CVE-2024-23275**	https://support.apple.com/en-us/HT214085	
Affected Version(s): From (including) 14.0 Up to (excluding) 14.4					
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23225**	https://support.apple.com/en-us/HT214081 , https://support.apple.com/en-us/HT214082 , https://support.apple.com/kb/HT214083 , https://support.apple.com/kb/HT214084 , https://support.apple.com/kb/HT214085 , https://support.apple.com/kb/HT214086	O-APP-MACO-200324/64
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel	https://support.apple.com/en-us/HT214081 , https://support.apple.com/kb/HT214084 , https://support.apple.com/kb/HT214086 ,	O-APP-MACO-200324/65

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
			memory protections. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23296**	https://support.apple.com/kb/HT214087, https://support.apple.com/kb/HT214088	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Mar-2024	7.8	An injection issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges. **CVE ID : CVE-2024-23268**	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/66
N/A	08-Mar-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.7.4, macOS Ventura 13.6.5, macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, tvOS 17.4. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23270**	https://support.apple.com/en-us/HT214081, https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085, https://suppo	O-APP-MACO-200324/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				rt.apple.com/en-us/HT214086	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Mar-2024	7.8	An injection issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges. **CVE ID : CVE-2024-23274**	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/68
N/A	08-Mar-2024	7.8	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges. **CVE ID : CVE-2024-23276**	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/69
N/A	08-Mar-2024	5.9	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4. An attacker in a privileged network position may be able to inject keystrokes by	https://support.apple.com/en-us/HT214081, https://support.apple.com/en-us/HT214084	O-APP-MACO-200324/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			spoofing a keyboard. **CVE ID : CVE-2024-23277**		
N/A	08-Mar-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2024-23266**	https://support.apple.com/en-us/HT214083 , https://support.apple.com/en-us/HT214084 , https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/71
N/A	08-Mar-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to bypass certain Privacy preferences. **CVE ID : CVE-2024-23267**	https://support.apple.com/en-us/HT214083 , https://support.apple.com/en-us/HT214084 , https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/72
N/A	08-Mar-2024	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. A user may gain access to	https://support.apple.com/en-us/HT214083 , https://support.apple.com/en-us/HT214084 ,	O-APP-MACO-200324/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected parts of the file system. **CVE ID : CVE-2024-23272**	https://support.apple.com/en-us/HT214085	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Mar-2024	4.7	A race condition was addressed with additional validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to access protected user data. **CVE ID : CVE-2024-23275**	https://support.apple.com/en-us/HT214083 , https://support.apple.com/en-us/HT214084 , https://support.apple.com/en-us/HT214085	O-APP-MACO-200324/74
N/A	08-Mar-2024	4.3	This issue was addressed through improved state management. This issue is fixed in Safari 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4. Private Browsing tabs may be accessed without authentication. **CVE ID : CVE-2024-23273**	https://support.apple.com/en-us/HT214081 , https://support.apple.com/en-us/HT214084 , https://support.apple.com/en-us/HT214089	O-APP-MACO-200324/75
Product: tvos					
Affected Version(s): * Up to (excluding) 17.4					
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS	https://support.apple.com/en-us/HT214081 , https://suppo	O-APP-TVOS-200324/76

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
			16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23225**	rt.apple.com/en-us/HT214082 , https://support.apple.com/kb/HT214083 , https://support.apple.com/kb/HT214084 , https://support.apple.com/kb/HT214085 , https://support.apple.com/kb/HT214086	
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23296**	https://support.apple.com/en-us/HT214081 , https://support.apple.com/kb/HT214084 , https://support.apple.com/kb/HT214086 , https://support.apple.com/kb/HT214087 , https://support.apple.com/kb/HT214088	O-APP-TVOS-200324/77
N/A	08-Mar-2024	7.8	The issue was addressed with improved memory	https://support.apple.com/en-	O-APP-TVOS-200324/78

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
			handling. This issue is fixed in macOS Monterey 12.7.4, macOS Ventura 13.6.5, macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, tvOS 17.4. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23270**	us/HT214081 , https://support.apple.com/en-us/HT214083 , https://support.apple.com/en-us/HT214084 , https://support.apple.com/en-us/HT214085 , https://support.apple.com/en-us/HT214086	
Product: visionos					
Affected Version(s): * Up to (excluding) 1.1					
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited.	https://support.apple.com/en-us/HT214081 , https://support.apple.com/en-us/HT214082 , https://support.apple.com/kb/HT214083 , https://support.apple.com/kb/HT214084 , https://support.apple.com/	O-APP-VISI-200324/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23225	kb/HT214085 , https://support.apple.com/kb/HT214086	
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23296**	https://support.apple.com/en-us/HT214081 , https://support.apple.com/kb/HT214084 , https://support.apple.com/kb/HT214086 , https://support.apple.com/kb/HT214087 , https://support.apple.com/kb/HT214088	O-APP-VISI-200324/80
Product: watchos					
Affected Version(s): * Up to (excluding) 10.4					
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass	https://support.apple.com/en-us/HT214081 , https://support.apple.com/en-us/HT214082 , https://support.apple.com/kb/HT214083 ,	O-APP-WATC-200324/81

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
			kernel memory protections. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23225**	https://support.apple.com/kb/HT214084, https://support.apple.com/kb/HT214085, https://support.apple.com/kb/HT214086	
Out-of-bounds Write	05-Mar-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23296**	https://support.apple.com/en-us/HT214081, https://support.apple.com/kb/HT214084, https://support.apple.com/kb/HT214086, https://support.apple.com/kb/HT214087, https://support.apple.com/kb/HT214088	O-APP-WATC-200324/82
Vendor: Fortinet					
Product: fortios					
Affected Version(s): 7.4.0					
Out-of-bounds Write	12-Mar-2024	9.8	A out-of-bounds write in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through	https://fortiguard.com/psirt/FG-IR-23-328	O-FOR-FORT-200324/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42789**		
Affected Version(s): 7.4.1					
Out-of-bounds Write	12-Mar-2024	9.8	A out-of-bounds write in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42789**	https://fortiguard.com/psirt/FG-IR-23-328	O-FOR-FORT-200324/84
Affected Version(s): From (including) 6.2.0 Up to (including) 6.2.15					
Out-of-bounds Write	12-Mar-2024	9.8	A out-of-bounds write in Fortinet FortiOS 7.4.0	https://fortiguard.com/psir	O-FOR-FORT-200324/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42789**	t/FG-IR-23-328	
Stack-based Buffer Overflow	12-Mar-2024	8.1	A stack-based buffer overflow in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42790**	https://fortiguard.com/psirt/FG-IR-23-327	O-FOR-FORT-200324/86
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.14					

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 Write	12-Mar-2024	9.8	A out-of-bounds write in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42789**	https://fortiguard.com/psirt/FG-IR-23-328	O-FOR-FORT-200324/87
Stack-based Buffer Overflow	12-Mar-2024	8.1	A stack-based buffer overflow in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.	https://fortiguard.com/psirt/FG-IR-23-327	O-FOR-FORT-200324/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42790		
Affected Version(s): From (including) 6.4.7 Up to (including) 6.4.14					
Authorization Bypass Through User-Controlled Key	12-Mar-2024	4.3	An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiOS version 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.1 through 7.0.13, 6.4.7 through 6.4.14, and FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 SSL-VPN may allow an authenticated attacker to gain access to another user's bookmark via URL manipulation. **CVE ID : CVE-2024-23112**	https://fortiguard.com/psirt/FG-IR-24-013	O-FOR-FORT-200324/89
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.12					
Out-of-bounds Write	12-Mar-2024	9.8	A out-of-bounds write in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0	https://fortiguard.com/psirt/FG-IR-23-328	O-FOR-FORT-200324/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42789**		
Stack-based Buffer Overflow	12-Mar-2024	8.1	A stack-based buffer overflow in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42790**	https://fortiguard.com/psirt/FG-IR-23-327	O-FOR-FORT-200324/91
Affected Version(s): From (including) 7.0.1 Up to (including) 7.0.13					
Authorization Bypass Through User-Controlled Key	12-Mar-2024	4.3	An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiOS version 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.1 through 7.0.13, 6.4.7 through	https://fortiguard.com/psirt/FG-IR-24-013	O-FOR-FORT-200324/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.4.14, and FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 SSL-VPN may allow an authenticated attacker to gain access to another user’s bookmark via URL manipulation. **CVE ID : CVE-2024-23112**		
Affected Version(s): From (including) 7.2.0 Up to (including) 7.2.5					
Out-of-bounds Write	12-Mar-2024	9.8	A out-of-bounds write in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42789**	https://fortiguard.com/psirt/FG-IR-23-328	O-FOR-FORT-200324/93
Stack-based Buffer Overflow	12-Mar-2024	8.1	A stack-based buffer overflow in Fortinet FortiOS 7.4.0 through 7.4.1,	https://fortiguard.com/psirt/FG-IR-23-327	O-FOR-FORT-200324/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42790**		
Affected Version(s): From (including) 7.2.0 Up to (including) 7.2.6					
Authorization Bypass Through User-Controlled Key	12-Mar-2024	4.3	An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiOS version 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.1 through 7.0.13, 6.4.7 through 6.4.14, and FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 SSL-VPN may allow an authenticated attacker to gain access to another user's bookmark via URL manipulation.	https://fortiguard.com/psirt/FG-IR-24-013	O-FOR-FORT-200324/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23112		
Affected Version(s): From (including) 7.4.0 Up to (including) 7.4.1					
Stack-based Buffer Overflow	12-Mar-2024	8.1	A stack-based buffer overflow in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE ID : CVE-2023-42790**	https://fortiguard.com/psirt/FG-IR-23-327	O-FOR-FORT-200324/96
Authorization Bypass Through User-Controlled Key	12-Mar-2024	4.3	An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiOS version 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.1 through 7.0.13, 6.4.7 through 6.4.14, and FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 SSL-VPN may allow an authenticated	https://fortiguard.com/psirt/FG-IR-24-013	O-FOR-FORT-200324/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to gain access to another user’s bookmark via URL manipulation. **CVE ID : CVE-2024-23112**		
Vendor: Qnap					
Product: qts					
Affected Version(s): * Up to (excluding) 4.5.4.2627					
Improper Authentication	08-Mar-2024	9.8	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the system via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QTS-200324/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QuTScloud c5.1.5.2651 and later **CVE ID : CVE-2024-21899**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Mar-2024	4.7	A SQL injection vulnerability has been reported to affect myQNAPcloud. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: myQNAPcloud 1.0.52 (2023/11/24) and later QTS 4.5.4.2627 build 20231225 and later **CVE ID : CVE-2024-21901**	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QTS-200324/99
Affected Version(s): * Up to (excluding) 5.1.3.2578					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	08-Mar-2024	6.5	An injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QTS-200324/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later **CVE ID : CVE-2024-21900**		
Affected Version(s): 4.5.4.2627					
Improper Authentication	08-Mar-2024	9.8	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the system via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QTS-200324/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later **CVE ID : CVE-2024-21899**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Mar-2024	4.7	A SQL injection vulnerability has been reported to affect myQNAPcloud. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: myQNAPcloud 1.0.52 (2023/11/24) and later QTS 4.5.4.2627 build 20231225 and later **CVE ID : CVE-2024-21901**	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QTS-200324/102
Affected Version(s): 5.1.3.2578					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Mar-2024	9.8	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the system via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later **CVE ID : CVE-2024-21899**	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QTS-200324/103
Improper Neutralization of Special Elements in Output	08-Mar-2024	6.5	An injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QTS-200324/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Used by a Downstream Component ('Injection')			exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later **CVE ID : CVE-2024-21900**		
Affected Version(s): From (including) 5.1.0 Up to (excluding) 5.1.3.2578					
Improper Authentication	08-Mar-2024	9.8	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the system via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QTS-200324/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.3.2578 build 20231110 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later **CVE ID : CVE-2024-21899**		
Product: qutscloud					
Affected Version(s): * Up to (excluding) c5.1.5.2651					
Improper Authentication	08-Mar-2024	9.8	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the system via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QUTS-200324/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later **CVE ID : CVE-2024-21899**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Mar-2024	6.5	An injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QUTS-200324/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21900		
Product: quts_hero					
Affected Version(s): * Up to (excluding) h4.5.4.2626					
Improper Authentication	08-Mar-2024	9.8	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the system via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later **CVE ID : CVE-2024-21899**	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QUTS-200324/108
Affected Version(s): * Up to (excluding) h5.1.3.2578					

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 in Output Used by a Downstream Component ('Injection')	08-Mar-2024	6.5	An injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later **CVE ID : CVE-2024-21900**	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QUTS-200324/109
Affected Version(s): From (including) h5.1.0 Up to (excluding) h5.1.3.2578					
Improper Authentication	08-Mar-2024	9.8	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QUTS-200324/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later **CVE ID : CVE-2024-21899**		
Affected Version(s): h4.5.4.2626					
Improper Authentication	08-Mar-2024	9.8	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the system via a network. We have already fixed the	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QUTS-200324/111

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later **CVE ID : CVE-2024-21899**		
Affected Version(s): h5.1.3.2578					
Improper Authentication	08-Mar-2024	9.8	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the system via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QUTS-200324/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.3.2578 build 20231110 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later **CVE ID : CVE-2024-21899**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Mar-2024	6.5	An injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later	https://www.qnap.com/en/security-advisory/qsa-24-09	O-QNA-QUTS-200324/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QuTScloud c5.1.5.2651 and later **CVE ID : CVE-2024-21900**		
Vendor: Tp-link					
Product: tl-sg2210p_firmware					
Affected Version(s): 5.0					
N/A	06-Mar-2024	8.8	TP-Link JetStream Smart Switch TL-SG2210P 5.0 Build 20211201 allows attackers to escalate privileges via modification of the 'tid' and 'usrlvl' values in GET requests. **CVE ID : CVE-2023-43318**	N/A	O-TP--TL-S-200324/114