CYBER ADVISORY

TLP:CLEAR
13 February 2024

QNAP Vulnerabilities

CVE-2023-47218 | CVE-2023-50358 | QNAP OS | High Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of high vulnerabilities, known as CVE-2023-47218 and CVE-2023-50358.[1] The vulnerabilities affect several QNAP operating system versions.[2] An unauthenticated attacker may exploit the quick.cgi component of QNAP QTS firmware, via command injection.[3]

Affected Version(s)	Fixed version
QTS 5.1.x	QTS 5.1.5.2645 build 20240116 and later
QTS 5.0.1	QTS 5.1.5.2645 build 20240116 and late
QTS 5.0.0	QTS 5.1.5.2645 build 20240116 and later
QTS 4.5.x, 4,4,x	QTS 4.5.4.2627 build 20231225 and later
QTS 4.3.6, 4.3.5	QTS 4.3.6.2665 build 20240131 and later
QTS 4.3.4	QTS 4.3.4.2675 build 20240131 and later
QTS 4.3.x	QTS 4.3.3.2644 build 20240131 and later
QTS 4.2.x	QTS 4.2.6 build 20240131 and later
QuTS hero h5.1.x	QuTS hero h5.1.5.2647 build 20240118 and later
QuTS hero h5.0.1	QuTS hero h5.1.5.2647 build 20240118 and later
QuTS hero h5.0.0	QuTS hero h5.1.5.2647 build 20240118 and later
QuTS hero h4.x	QuTS hero h4.5.4.2626 build 20231225 and later
QuTScloud c5.x	QuTScloud c5.1.5.2651 and later

Table 1: QNAP Affected Versions and Upgraded Versions

The Cal-CSIC recommends applying appropriated upgrades when possible.

For further information on applying upgrades, please refer to QNAP Product Support.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] QNAP; "QSA-23-57;" https://www.qnap.com/en/security-advisory/qsa-23-57; accessed 13 February 2024
[2] Unit42; "New Vulnerability in QNAP QTS Firmware: CVE-2023-50358;" https://unit42.paloaltonetworks.com/qnap-qts-firmware-cve-2023-50358/; accessed 13 February 2024
[3] Vulners; "CVE-2023-50358;" https://vulners.com/cve/CVE-2023-50358; accessed 13 February 2024