CYBER ADVISORY

TLP:CLEAR

08 March 2024

Multiple QNAP NAS Services Vulnerabilities

CVE-2024-21899 | CVE-2024-21900 | CVE-2024-21901 | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of critical vulnerabilities, known as CVE-2024-21899, CVE-2024-21900, and CVE-2024-21901.[1] The vulnerabilities affect QNAP products QTS, QuTS hero, QuTScloud, and myQNAPcloud.[2] CVE-2024-21899 is an improper authentication vulnerability which may allow an attacker to compromise the security of the system via a network. CVE-2024-21900 is an injection vulnerability which could allow an authenticated attacker to execute commands via a network. CVE-2024-21901 is a SQL injection vulnerability which could allow an authenticated attacker with administrator access to inject malicious code via a network. [3]

Affected Product	Fixed version
QTS 5.1.x	QTS 5.1.3.2578 build 20231110 and later
QTS 4.5.x	QTS 4.5.4.2627 build 20231225 and later
QuTS hero h5.1.x	QuTS hero h5.1.3.2578 build 20231110 and later
QuTS hero h4.5.x	QuTS hero h4.5.4.2626 build 20231225 and later
QuTScloud c5.x	QuTScloud c5.1.5.2651 and later
myQNAPcloud 1.0.x	myQNAPcloud 1.0.52 (2023/11/24) and later

Table 1: QNAP Affected Products and Upgraded Versions

The Cal-CSIC recommends immediately applying the appropriated product upgrade.

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-24-09;" https://www.qnap.com/en/security-advisory/qsa-24-09; accessed 08 March 2024
[2] Bleeping Computer; "QNAP warns of critical auth bypass flaw in its NAS devices;" https://www.bleepingcomputer.com/news/security/qnap-warns-of-critical-auth-bypass-flaw-in-its-nas-devices/; accessed 08 March 2024
[3] Vulnera; "QNAP Alerts Users about Critical Authentication Bypass Vulnerability in NAS Devices;" https://vulnera.com/newswire/qnap-alerts-users-about-critical-authentication-bypass-vulnerability-in-nas-devices/; accessed 08 March 2024