CYBER ADVISORY

TLP:CLEAR
22 May 2024

QNAP QTS and QuTS Vulnerabilities

QNAP | QTS | QuTS hero | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of critical vulnerabilities known as CVE-2024-21902, CVE-2024-27127, CVE-2024-27128, CVE-2024-27129, and CVE-2024-27130.[1] These vulnerabilities lie in QNAP's QTS 5.1.x and QuTS hero h5.1.x.[2] Exploitation of CVE-2024-21902 could allow authenticated users to read or modify the resource via a network. Exploitation of CVE-2024-27127 could allow authenticated users to execute arbitrary code via a network. Exploitation of CVE-2024-27128, CVE-2024-27129, and CVE-2024-27130 could allow authenticated users to execute arbitrary code via a network.[3,4]

The Cal-CSIC recommends to immediately upgrade to the appropriate patched QNAP product.

For further information on applying Veeam updates, 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] Help Net Security; "15 QNAP NAS bugs and one PoC disclosed, update ASAP! (CVE-2024-27130);" https://www.helpnetsecurity.com/2024/05/21/cve-2024-27130-poc/; accessed 22 May 2024

[2] Bleeping Computer; "QNAP QTS zero-day in Share feature gets public RCE exploit;" https://www.bleepingcomputer.com/news/security/qnap-qts-zero-day-in-share-feature-gets-public-rce-exploit/; accessed 22 May 2024

[3] Watch Tower Labs; "QNAP QTS - QNAPping At The Wheel (CVE-2024-27130 and friends);" https://labs.watchtowr.com/qnap-qts-qnapping-at-the-wheel-cve-2024-27130-and-friends/; accessed 22 May 2024

[4] QNAP; "Security ID : QSA-24-23 Vulnerabilities in QTS and QuTS hero;" https://www.qnap.com/en/security-advisory/qsa-24-23; accessed 22 May 2024