مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in QNAP Products

Tracking #:432315688

Date:11-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in QNAP products that could be exploited to gain unauthorized access on affected systems.

TECHNICAL DETAILS:

Critical Vulnerabilities Details:

- **CVE-2024-21899**
  - An improper authentication vulnerability exists in the QNAP operating system. A successful exploitation of this vulnerability could allow attackers to compromise the security of the system via a network.
- **CVE-2024-21900**
  - An injection vulnerability exists in the QNAP operating system. A successful exploitation of this vulnerability could allow authenticated users to execute commands via a network.
- **CVE-2024-21901**
  - A SQL injection vulnerability exists in myQNAPcloud. A successful exploitation of this vulnerability could allow authenticated administrators to inject malicious code via a network.

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

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by QNAP.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://www.qnap.com/en-me/security-advisory/qsa-24-09