مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in QNAP Notes Station 3

Tracking #:432316558

Date:26-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed QNAP has disclosed multiple critical vulnerabilities in Notes Station 3, a note-taking and collaboration application used in QNAP NAS systems.

TECHNICAL DETAILS:

QNAP has disclosed multiple critical vulnerabilities in Notes Station 3, a note-taking and collaboration application used in QNAP NAS systems. These vulnerabilities, identified as CVE-2024-38643, CVE-2024-38644, CVE-2024-38645, and CVE-2024-38646, affect versions 3.9.x and have been resolved in version 3.9.7 and later. The most severe vulnerability (CVE-2024-38643) has a CVSS v4 score of 9.3, allowing remote attackers to gain unauthorized access and execute specific system functions without authentication.

- CVE-2024-38643 (CVSS 9.3): A missing authentication for critical function vulnerability. If exploited, this could allow remote attackers to gain unauthorized system access.
- CVE-2024-38644 (CVSS 8.7): A command injection vulnerability. Attackers with user access could execute arbitrary commands on the system.
- CVE-2024-38645 (CVSS 9.4): A server-side request forgery (SSRF) vulnerability. This flaw could enable attackers with user access to read application data.
- CVE-2024-38646 (CVSS 8.4): An incorrect permission assignment for critical resources. Local attackers with administrator access could gain unauthorized access to sensitive data.

- **Affected Versions:** Notes Station 3 version 3.9.x

- **Fixed Versions:** Notes Station 3 version 3.9.7 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to Update Notes Station 3 to the latest version.

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-au/security-advisory/qsa-24-36