

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



High-Severity Vulnerability in QNAP Helpdesk
Tracking #:432316951
Date:10-03-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability has been identified in QNAP's Helpdesk application, if exploited, could allow remote attackers to compromise system security.

TECHNICAL DETAILS:

A security vulnerability (CVE-2024-50394) has been identified in Helpdesk version 3.3.x. The vulnerability arises due to improper certificate validation, which could allow remote attackers to compromise the security of affected systems. Exploiting this flaw could enable attackers to intercept sensitive data, launch man-in-the-middle (MITM) attacks, or manipulate system communications.

- **CVE Identifier:** CVE-2024-50394
- **Severity:** High (CVSSv3 score: 7.7)
- **Affected Product:** QNAP Helpdesk version 3.3.x
- **Fixed Version:** Helpdesk 3.3.3 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade all instances of Helpdesk to fixed version or later.

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/security-advisory/qa-25-05>