مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in QNAP HBS 3 Hybrid Backup Sync

Tracking #:432316452

Date:30-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical zero-day vulnerability has been identified in QNAP's HBS 3 Hybrid Backup Sync, if exploited this vulnerability enables remote attackers to execute arbitrary commands on affected NAS devices.

TECHNICAL DETAILS:

Vulnerability Details:

- Vulnerability ID: **CVE-2024-50388**
- Severity: Critical
- Vulnerability Type: OS Command Injection
- Impact: Allows attackers to bypass input validation and execute arbitrary commands with system-level privileges. This could potentially lead to:
  - Unauthorized data access or exfiltration
  - Installation of malware or ransomware
  - Lateral movement within the network
  - Denial of service attacks

Affected Versions:

- HBS 3 Hybrid Backup Sync 25.1.x

Fixed Versions:

- HBS 3 Hybrid Backup Sync 25.1.1.673 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommend updating HBS 3 Hybrid Backup Sync 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/security-advisory/qsa-24-41