مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates-QNAP Products

Tracking #:432317776

Date:06-10-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed QNAP Systems, Inc. has released a security advisory addressing multiple vulnerabilities affecting two of its widely deployed utilities — NetBak Replicator and Qsync Central.

TECHNICAL DETAILS:

QNAP Systems, Inc. has released a security advisory addressing multiple vulnerabilities affecting two of its widely deployed utilities — NetBak Replicator and Qsync Central. The most severe issues, with CVSS scores reaching 8.6, could enable attackers to execute unauthorized code, disrupt NAS operations, or steal sensitive data.

Vulnerability Details

- CVE-2025-57714 – Code Execution in NetBak Replicator-An unquoted search path or element vulnerability allows local attackers to inject and execute malicious code by placing rogue executables in paths referenced by the software.
- CVE-2025-44012: Allocation of resources without limits or throttling vulnerability If a remote attacker gains access to a user account, they can then exploit the vulnerability to prevent other systems, applications, or processes from accessing the same type of resource.
- CVE-2025-47210: NULL pointer dereference vulnerability If a remote attacker gains access to a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack.
- CVE-2025-52867: Uncontrolled resource consumption vulnerability If a remote attacker gains access to a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack.
- CVE-2025-53595, CVE-2025-54153: SQL injection vulnerabilities If a remote attacker gains access to a user account, they can then exploit the vulnerabilities to execute unauthorized code or commands

Affected Product	Fixed Version
NetBak Replicator 4.5.x	NetBak Replicator 4.5.15.0807 and later
Qsync Central 5.0.0	Qsync Central 5.0.0.2 (2025/07/31) and later

RECOMMENDATIONS:

- Update Immediately: Upgrade NetBak Replicator & Qsync Central 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.

REFERNCES:

- https://www.qnap.com/en/security-advisory/qsa-25-39
- https://www.qnap.com/en/security-advisory/qsa-25-35