

مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Critical .NET Vulnerability Impacts QNAP NAS Backup Utility**

Tracking #:432317868

Date:28-10-2025

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed QNAP has confirmed that its NetBak PC Agent, a Windows-based backup utility for NAS devices, is impacted due to a critical vulnerability disclosed in Microsoft ASP.NET Core (.NET framework).

## TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-55315) in Microsoft ASP.NET Core (.NET framework) has been disclosed, carrying a CVSS score of 9.8. The flaw enables attackers to perform HTTP request smuggling, potentially resulting in credential theft, unauthorized access, and data manipulation within affected applications.

QNAP has confirmed that its NetBak PC Agent, a Windows-based backup utility for NAS devices, is impacted due to its dependency on the vulnerable ASP.NET Core runtime. This makes QNAP systems susceptible to credential interception and other attack vectors if not promptly updated.

The vulnerability underscores the broader risks posed by third-party software components that rely on shared frameworks like .NET. QNAP strongly advises all users to update their ASP.NET Core runtime to version 8.0.21 or later and reinstall the latest NetBak PC Agent to mitigate potential exploitation.

### Vulnerability Details

- **CVE ID:** CVE-2025-55315
- **Severity:** Critical (CVSS 9.8)
- **Affected Component:** Microsoft ASP.NET Core
- **Affected Product:** QNAP NetBak PC Agent for Windows

### Affected Versions

- QNAP NetBak PC Agent versions using ASP.NET Core runtime prior to v8.0.21.
- Systems where ASP.NET Core Hosting Bundle has not been updated since October 2025.

### Mitigation:

Users must ensure their systems are running the latest ASP.NET Core runtime version.

- Latest Secure Version: ASP.NET Core 8.0.21 (as of October 2025).

## RECOMMENDATIONS:

- Download the latest version from the official QNAP NetBak PC Agent download page or manually Update ASP.NET Core Runtime (Hosting Bundle).

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-25-44>