

POSTING DATE: 2026/01/14

[VULNERABILITY ALERT] QNAP NAS Applications Contain High-Risk Security Vulnerabilities (CVE-2025-59384 and CVE-2025-59387), Please Verify and Patch Immediately

- Subject: [VULNERABILITY ALERT] QNAP NAS Applications Contain High-Risk Security Vulnerabilities (CVE-2025-59384 and CVE-2025-59387), Please Verify and Patch Immediately
- Content Description:
 - Forwarded from National Information Security Information Sharing and Analysis Center Security Alert NISAC-200-202601-00000099
 - Researchers have discovered high-risk security vulnerabilities in QNAP NAS applications. Please verify and patch as soon as possible.
 - 1. Qfiling contains a Path Traversal vulnerability (CVE-2025-59384). A remote unauthenticated attacker can exploit this vulnerability to read unauthorized files or system data.
 - 2. MARS (Multi-Application Recovery Service) contains a SQL Injection vulnerability (CVE-2025-59387). A remote unauthenticated attacker can inject and execute unauthorized commands.
- Affected Platforms:
 - Qfiling versions 3.13.x prior to 3.13.1
 - MARS versions 1.2.x prior to 1.2.1.1686
- Recommended Actions:
 - The vendor has released security updates for these vulnerabilities. Please refer to the official advisories for updates at the following URLs:
 - <https://www.qnap.com/en/security-advisory/qs-a-25-54>
 - <https://www.qnap.com/en/security-advisory/qs-a-25-53>
- Reference Material:
 1. <https://nvd.nist.gov/vuln/detail/CVE-2025-59384>
 2. <https://nvd.nist.gov/vuln/detail/CVE-2025-59387>
 3. <https://www.qnap.com/en/security-advisory/qs-a-25-54>
 4. <https://www.qnap.com/en/security-advisory/qs-a-25-53>

Computer and Communication Center
Network Systems Division, Respectfully

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260114_07



Last update: **2026/01/14 14:18**