Post Date: 2026/06/30

□Vulnerability Alert□High-Risk Security Vulnerabilities (CVE-2026-23918, CVE-2026-29167, and CVE-2026-44631) Identified in Apache HTTP Server—Please Verify and Patch Immediately

- Subject: □Vulnerability Alert□High-Risk Security Vulnerabilities (CVE-2026-23918, CVE-2026-29167, and CVE-2026-44631) Identified in Apache HTTP Server—Please Verify and Patch Immediately

- Description:
  - Forwarded from National Information Security Analysis and Sharing Center (NISAC) Cybersecurity Alert: NISAC-200-202606-00000013
  - Researchers have discovered three high-risk security vulnerabilities (CVE-2026-23918, CVE-2026-29167, and CVE-2026-44631) in Apache HTTP Server. These include Double Free, Use After Free, and Buffer Overflow vulnerabilities. At their most severe, they could allow authenticated remote attackers to execute arbitrary code. Please verify your systems and apply patches as soon as possible.
- Affected Platforms:
  - Apache HTTP Server 2.4.66
  - Apache HTTP Server 2.4.0 to 2.4.67
- Recommended Actions:
  - Official fixes and updates have been released. Please refer to the official advisory to perform updates at the following URL: https://httpd.apache.org/security/vulnerabilities_24.html
- References:
  1. https://httpd.apache.org/security/vulnerabilities_24.html
  2. https://nvd.nist.gov/vuln/detail/CVE-2026-23918
  3. https://nvd.nist.gov/vuln/detail/CVE-2026-29167
  4. https://nvd.nist.gov/vuln/detail/CVE-2026-44631

Computer and Communication Center
Network Systems Division

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260630_21

Last update: **2026/06/30 09:10**