Posting Date: 2026/08/13

【Vulnerability Alert】CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/08/03-2026/08/09)

- Subject: 【Vulnerability Alert】CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/08/03-2026/08/09)

- Description:
  - Forwarded Cybersecurity Alert from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202608-00000009
  - 【CVE-2026-18556】N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v4.0: 8.2)
  - 【Ransomware Use: Unknown】 An authentication bypass vulnerability exists in N-able N-central, allowing attackers to bypass authentication mechanisms using an alternate path or channel.
  - 【CVE-2026-18577】N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v4.0: 8.2)
  - 【Ransomware Use: Unknown】 An authentication bypass vulnerability exists in N-able N-central, allowing attackers to bypass authentication mechanisms via an alternate path or channel and subsequently take over accounts in N-central. This vulnerability stems from an incomplete patch issued for CVE-2026-18556.
  - 【CVE-2026-34486】Apache Tomcat Missing Encryption of Sensitive Data Vulnerability (CVSS v3.1: 7.5)
  - 【Ransomware Use: Unknown】 A missing encryption of sensitive data vulnerability exists in Apache Tomcat, allowing attackers to exploit it to bypass EncryptInterceptor. This vulnerability can be chained with CVE-2025-24813.
  - 【CVE-2026-9198】IBM Langflow Code Injection Vulnerability (CVSS v3.1: 9.8)
  - 【Ransomware Use: Unknown】 A code injection vulnerability exists in Langflow, allowing unauthenticated attackers to achieve full remote code execution in default Langflow deployment environments.
  - 【CVE-2026-63077】JetBrains TeamCity Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.8)
  - 【Ransomware Use: Unknown】 A deserialization of untrusted data vulnerability exists in JetBrains TeamCity, allowing attackers to execute remote code unauthenticated via the agent polling protocol.
  - 【CVE-2026-8037】Progress LoadMaster Command Injection Vulnerability (CVSS v3.1: 9.6)
  - 【Ransomware Use: Unknown】 A command injection vulnerability exists in Progress LoadMaster, allowing unauthenticated attackers to execute arbitrary commands on LoadMaster devices by leveraging unsanitized inputs across multiple command endpoints.
- Affected Systems:
  - 【CVE-2026-18556】 Please refer to the affected versions listed on the official page: https://uptime.n-able.com/event/201522/
  - 【CVE-2026-18577】 Please refer to the affected versions listed on the official page: https://uptime.n-able.com/event/201522/

    - 【CVE-2026-34486】 Please refer to the affected versions listed on the official page: https://lists.apache.org/thread/9510k5p5zdvt9pkkgtyp85mvwxo2qrly
    - 【CVE-2026-9198】 Please refer to the affected versions listed on the official page: https://www.ibm.com/support/pages/node/7278927
    - 【CVE-2026-63077】 JetBrains TeamCity versions prior to 2026.1.3 and 2025.11.7
    - 【CVE-2026-8037】 Please refer to the affected versions listed on the official page: https://community.progress.com/s/article/LoadMaster-Critical-Security-Bulletin-June-2026-CVE-2026-8037-CVE-2026-33691
- Recommendations:
    - 【CVE-2026-18556】 The vendor has released fix updates for the vulnerability; please update to the relevant versions: https://uptime.n-able.com/event/201522/
    - 【CVE-2026-18577】 The vendor has released fix updates for the vulnerability; please update to the relevant versions: https://uptime.n-able.com/event/201522/
    - 【CVE-2026-34486】 The vendor has released fix updates for the vulnerability; please update to the relevant versions: https://lists.apache.org/thread/9510k5p5zdvt9pkkgtyp85mvwxo2qrly
    - 【CVE-2026-9198】 The vendor has released fix updates for the vulnerability; please update to the relevant versions: https://www.ibm.com/support/pages/node/7278927
    - 【CVE-2026-63077】 The vendor has released fix updates for the vulnerability; please update to the relevant versions: https://www.jetbrains.com/privacy-security/issues-fixed/
    - 【CVE-2026-8037】 The vendor has released fix updates for the vulnerability; please update to the relevant versions: https://community.progress.com/s/article/LoadMaster-Critical-Security-Bulletin-June-2026-CVE-2026-8037-CVE-2026-33691

Computer and Communication Center
Network System Division

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260813_21

Last update: **2026/08/13 14:00**