Post Date: 2026/06/17

【Vulnerability Alert】CISA Adds 7 Known Exploited Vulnerabilities to KEV Catalog (2026/06/08-2026/06/14)

- Subject: 【Vulnerability Alert】CISA Adds 7 Known Exploited Vulnerabilities to KEV Catalog (2026/06/08-2026/06/14)

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center Security Alert TWCERTCC-200-202606-00000011
  1. 【CVE-2026-42271】BerriAI LiteLLM Command Injection Vulnerability (CVSS v3.1: 8.8)
     - 【Exploited by Ransomware: Unknown】 A command injection vulnerability exists in BerriAI LiteLLM, which could allow any authenticated user (including those holding only low-privileged internal user keys) to execute arbitrary commands on the host.
     - 【Affected Platforms】Please refer to the affected versions listed by the official advisory
     - https://github.com/BerriAI/litellm/security/advisories/GHSA-v4p8-mg3p-g94g
  2. 【CVE-2026-50751】Check Point Security Gateway Improper Authentication Vulnerability (CVSS v3.1: 9.3)
     - 【Exploited by Ransomware: Known】 An improper authentication vulnerability exists in the IKEv1 key exchange mechanism of Check Point Security Gateway, which could allow an unauthenticated remote attacker to bypass authentication mechanisms and establish a remote access VPN connection without possessing valid user credentials.
     - 【Affected Platforms】Please refer to the affected versions listed by the official advisory
     - https://support.checkpoint.com/results/sk/sk185033

1. 【CVE-2026-11645】Google Chromium V8 Out-of-Bounds Read and Write Vulnerability (CVSS v3.1: 8.8)
   - 【Exploited by Ransomware: Unknown】 An out-of-bounds read and write vulnerability exists in Google Chromium V8. A remote attacker could execute arbitrary code within the sandbox via a specially crafted HTML page. This vulnerability may affect various web browsers using the Chromium core, including but not limited to Google Chrome, Microsoft Edge, and Opera.
   - 【Affected Platforms】Please refer to the affected versions listed by the official advisory
   - https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
2. 【CVE-2026-7473】Arista Extensible Operating System Incomplete Comparison with Missing Factors Vulnerability (CVSS v3.1: 5.8)
   - 【Exploited by Ransomware: Unknown】 An Incomplete Comparison with Missing Factors vulnerability exists in Arista Extensible Operating System. When a switch receives an unexpected tunneled packet whose destination IP address matches its configured decapsulation IP, it may incorrectly perform decapsulation and forward it, leading to

unexpected traffic handling behavior.
    - Affected Platforms：Please refer to the affected versions listed by the official advisory
    - https://www.arista.com/en/support/advisories-notices/security-advisory/24005-security-advisory-0137

1. CVE-2026-20245：Cisco Catalyst SD-WAN Manager Improper Encoding or Escaping of Output Vulnerability (CVSS v3.1: 7.8)
    - Exploited by Ransomware: Unknown： An Improper Encoding or Escaping of Output vulnerability exists in Cisco Catalyst SD-WAN Manager. This vulnerability could allow an authenticated local attacker to execute arbitrary commands with root privileges by providing a specially crafted file to the affected system.
    - Affected Platforms：Please refer to the affected versions listed by the official advisory
    - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx
2. CVE-2026-10520：Ivanti Sentry OS Command Injection Vulnerability (CVSS v3.1: 10.0)
    - Exploited by Ransomware: Unknown： An operating system command injection vulnerability exists in Ivanti Sentry, which could allow an unauthenticated remote user to execute remote code with root privileges. An attacker can successfully exploit this vulnerability when the Sentry appliance is in an unmanaged state and its endpoints are accessible from the external network. If mTLS is used with EPMM, or HTTPS access is restricted through Neurons for MDM, external attackers will be prevented from accessing the relevant interfaces.
    - Affected Platforms：Please refer to the affected versions listed by the official advisory
    - https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-10520-CVE-2026-10523

1. CVE-2026-35273：Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 9.8)
    - Exploited by Ransomware: Known： A missing authentication for critical function vulnerability exists in Oracle PeopleSoft Enterprise PeopleTools. An unauthenticated attacker could exploit this vulnerability to gain control of PeopleSoft Enterprise PeopleTools.
    - Affected Platforms：Please refer to the affected versions listed by the official advisory https://www.oracle.com/security-alerts/alert-cve-2026-35273.html

- Affected Platforms:
    - Detailed information is listed under the Affected Platforms section within the Description field.
- Recommended Actions:
    1. CVE-2026-42271： The vendor has released a security patch for this vulnerability, please update to the relevant version.
        - https://github.com/BerriAI/litellm/security/advisories/GHSA-v4p8-mg3p-g94g
    2. CVE-2026-50751： The vendor has released a security patch for this vulnerability, please update to the relevant version.
        - https://support.checkpoint.com/results/sk/sk185033
    3. CVE-2026-11645： The vendor has released a security patch for this vulnerability, please update to the relevant version.
        - https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
    4. CVE-2026-7473： The vendor has released a security patch for this vulnerability, please update to the relevant version.

- https://www.arista.com/en/support/advisories-notices/security-advisory/24005-security-advisory-0137

1. CVE-2026-20245 The vendor has released a security patch for this vulnerability, please update to the relevant version.

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx

1. CVE-2026-10520 The vendor has released a security patch for this vulnerability, please update to the relevant version.

- https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-10520-CVE-2026-10523

1. CVE-2026-35273 The vendor has released a security patch for this vulnerability, please update to the relevant version.

- https://www.oracle.com/security-alerts/alert-cve-2026-35273.html

---

Computer and Communication Center
Network Systems Division