Date Posted: 2026/08/07

【Vulnerability Alert】CISA Adds 3 Known Exploited Vulnerabilities to KEV Catalog (2026/07/27-2026/08/02)

- Subject: 【Vulnerability Alert】CISA Adds 3 Known Exploited Vulnerabilities to KEV Catalog (2026/07/27-2026/08/02)

- Description:
  - Forwarded Security Alert from TWCERT/CC (Taiwan Computer Emergency Response Team/Coordination Center) TWCERTCC-200-202608-00000001
  - 【CVE-2025-68686】Fortinet FortiOS Exposure of Sensitive Information to an Unauthorized Actor Vulnerability (CVSS v3.1: 5.9)
  - 【Known Ransomware Use: Unknown】 Fortinet FortiOS contains an Exposure of Sensitive Information to an Unauthorized Actor vulnerability that may allow an unauthorized remote attacker to bypass patches developed for symlink persistence mechanisms observed in post-exploitation scenarios via crafted HTTP requests. An attacker must first successfully compromise the product via other system-level vulnerabilities to exploit this vulnerability.
  - 【CVE-2026-16812】Arista VeloCloud Orchestrator On-Prem OS Command Injection Vulnerability (CVSS v3.1: 10.0)
  - 【Known Ransomware Use: Unknown】 Arista VeloCloud Orchestrator On-Prem contains an OS command injection vulnerability that may allow a remote attacker to access internal privileged functionality and impact the VCO host. Successful exploitation could compromise the confidentiality, integrity, and availability of the Orchestrator and the data it manages.
  - 【CVE-2026-20316】Cisco Secure Firewall Management Center Use of Hard-coded Password Vulnerability (CVSS v3.1: 5.3)
  - 【Known Ransomware Use: Unknown】 Cisco Secure Firewall Management Center contains a use of hard-coded password vulnerability that may allow an unauthenticated remote attacker to log in to an affected device using a low-privileged account and access sensitive data within the affected system.
- Affected Platforms:
  - 【CVE-2025-68686】 Please refer to the official vendor advisory for affected versions: https://fortiguard.fortinet.com/psirt/FG-IR-25-934
  - 【CVE-2026-16812】 Please refer to the official vendor advisory for affected versions: https://www.arista.com/en/support/advisories-notices/security-advisory/24364-security-advisory-0144
  - 【CVE-2026-20316】 Please refer to the official vendor advisory for affected versions: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh
- Recommendations:
  - 【CVE-2025-68686】 The vendor has released security patches for this vulnerability. Please update to the relevant version: https://fortiguard.fortinet.com/psirt/FG-IR-25-934
  - 【CVE-2026-16812】 The vendor has released security patches for this vulnerability. Please update to the relevant version:

https://www.arista.com/en/support/advisories-notices/security-advisory/24364-security-advisory-0144
- CVE-2026-20316 The vendor has released security patches for this vulnerability. Please update to the relevant version: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh

---

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:20260807_21

Last update: **2026/08/07 09:19**