Date Posted: 2026/03/03

[Vulnerability Alert] CISA Adds 3 Known Exploited Vulnerabilities to KEV Catalog (2026/02/23-2026/03/01)

- Subject Explanation: [Vulnerability Alert] CISA Adds 3 Known Exploited Vulnerabilities to KEV Catalog (2026/02/23-2026/03/01)

- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202603-00000001
  - [CVE-2026-25108] Soliton Systems K.K FileZen OS Command Injection Vulnerability (CVSS v3.1: 8.8)
  - [Ransomware Exploitation: Unknown] Soliton Systems K.K FileZen contains an OS command injection vulnerability. This vulnerability can be triggered when a user logs into the affected product and sends a specially crafted HTTP request.
  - [CVE-2022-20775] Cisco SD-WAN Path Traversal Vulnerability (CVSS v3.1: 7.8)
  - [Ransomware Exploitation: Unknown] A path traversal vulnerability exists in the Cisco SD-WAN CLI. Due to improper command access control within the application CLI, an authenticated local attacker could exploit this to escalate privileges. Upon successful exploitation, an attacker could execute arbitrary commands as the root user.
  - [CVE-2026-20127] Cisco Catalyst SD-WAN Controller and Manager Authentication Bypass Vulnerability (CVSS v3.1: 10.0)
  - [Ransomware Exploitation: Unknown] Cisco Catalyst SD-WAN Controller (formerly SD-WAN vSmart) and Cisco Catalyst SD-WAN Manager (formerly SD-WAN vManage) contain an authentication bypass vulnerability. This could allow an unauthenticated remote attacker to bypass authentication mechanisms and gain administrative privileges on the affected system.
- Impacted Platforms:
  - [CVE-2026-25108] Please refer to the official list of affected versions: https://www.soliton.co.jp/support/2026/006657.html
  - [CVE-2022-20775] Please refer to the official list of affected versions: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-priv-E6e8tEdF
  - [CVE-2026-20127] Please refer to the official list of affected versions: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk
- Suggested Measures:
  - [CVE-2026-25108] Official fix updates have been released. Please update to the relevant version: https://www.soliton.co.jp/support/2026/006657.html
  - [CVE-2022-20775] Official fix updates have been released. Please update to the relevant version: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-priv-E6e8tEdF
  - [CVE-2026-20127] Official fix updates have been released. Please update to the relevant

version:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk

---

Computer and Communication Center
Network Systems Division