مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Cisco ClamAV

Tracking #:432319234

Date:03-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Cisco has released a security advisory addressing multiple high-severity vulnerabilities in the ClamAV antivirus engine used by Cisco Secure Endpoint Connector.

TECHNICAL DETAILS:

Cisco has released a security advisory addressing multiple high-severity vulnerabilities in the ClamAV antivirus engine used by Cisco Secure Endpoint Connector. The vulnerabilities may allow an unauthenticated remote attacker to trigger Denial-of-Service (DoS) conditions by submitting specially crafted files for scanning. On Windows platforms, exploitation may terminate the ClamAV scanning process, potentially rendering the endpoint unresponsive and requiring manual recovery.

Vulnerability Details

- CVE-2026-20213 – PE File Processing Memory Corruption
  - CVSS: 7.5 (High)
- CVE-2026-20214 – FSG File Processing Memory Corruption
  - CVSS: 7.5 (High)
- CVE-2026-20215 – 7z File Processing Memory Corruption
  - CVSS: 7.5 (High)
- CVE-2026-20216 – InstallShield File Parsing Denial-of-Service (DoS)
  - CVSS: 7.5 (High)
- CVE-2026-20217 – PESpin File Processing Memory Corruption
  - CVSS: 7.5 (High)
- CVE-2026-20243 – ALZ File Processing Memory Corruption
  - CVSS: 7.5 (High)
- CVE-2026-20244 – DMG File Processing Memory Corruption
  - CVSS: 7.5 (High)

Affected Products:

Product	Impact	Fixed Version
Secure Endpoint Connector for Windows	High	8.6.2
Secure Endpoint Connector for Linux	Medium	1.29.0
Secure Endpoint Connector for Mac	Medium	1.27.2

RECOMMENDATIONS:

Immediate Actions:

- Upgrade Cisco Secure Endpoint Connector to the latest fixed release.
- Prioritize Windows endpoints due to their higher security impact.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyxR