Public Exploits Released for ClamAV Vulnerabilities Affecting Cisco Secure Endpoint

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

Public proof-of-concept exploit code is now available for an out-of-bounds write vulnerability (CVE-2026-20337) and a memory corruption vulnerability (CVE-2026-20338) affecting ClamAV and Cisco Secure Endpoint Connector.

An unauthenticated attacker could exploit either vulnerability with a crafted ZIP file, causing the ClamAV scanning process to terminate.

Overview

There are two high-severity vulnerabilities in the ClamAV ZIP archive parser that could allow an unauthenticated, remote attacker to cause a denial-of-service condition. ClamAV is an open-source antivirus engine used to scan files for malware and is included in Cisco Secure Endpoint Connector.

- **CVE-2026-20337, CVSS 7.5** – An out-of-bounds write vulnerability caused by improper boundary checks when ClamAV processes ZIP files. A specially crafted ZIP file could terminate the scanning process.
- **CVE-2026-20338, CVSS 7.5** – A memory corruption vulnerability caused by improper memory handling when ClamAV processes ZIP files. A malformed archive could trigger a double-free condition and terminate the scanning process.

The vulnerabilities can be exploited independently and do not require authentication or user interaction. Public proof-of-concept code is available for both vulnerabilities, but exploitation has not been confirmed.

There are five additional ClamAV vulnerabilities in the same advisory. This notice focuses on CVE-2026-20337 and CVE-2026-20338 because public exploit code is available for both.

The security impact is rated high on Windows because the ClamAV scanning process runs with elevated privileges. Cisco rates the impact as medium on Linux and macOS, where the process runs with fewer privileges.

Affected Products

- ClamAV versions 1.5.0 through 1.5.3
- Cisco Secure Endpoint Connector for Windows

- Cisco Secure Endpoint Connector for Linux
- Cisco Secure Endpoint Connector for Mac

Cisco Secure Endpoint Private Cloud is not directly vulnerable. However, the connector software distributed to endpoints is affected. Private Cloud versions 4.2.8 and later will support the corrected connector software when Cisco makes it available.

Aspire Protects

- **Patch** - Upgrade standalone ClamAV installations to version 1.5.4, which fixes both vulnerabilities. See Cisco's advisory for more information.
- Prepare for Cisco connector updates – Monitor the Cisco Secure Endpoint portal and deploy the corrected Connector release when it becomes available. Cisco expects to release updates in August 2026, but fixed version numbers have not been published.
- Verify automatic update settings – Review Secure Endpoint policies to confirm Connector updates are enabled and endpoints are receiving current software.
- Monitor scanning operations – Investigate unexpected ClamAV process termination, repeated scan failures or scanning errors involving ZIP archives.

TTPs to Watch

Impact

- Endpoint Denial of Service: Application or System Exploitation (T1499.004) – An attacker could exploit CVE-2026-20337 or CVE-2026-20338 by submitting a crafted ZIP file for scanning. Successful exploitation could terminate the ClamAV scanning process and interrupt malware scanning operations.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Any organization using affected ClamAV or Cisco Secure Endpoint Connector versions may be at risk, including:

- Government
- Technology

- Healthcare
- Finance
- Education
- Retail
- Manufacturing

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

ClamAV Vulnerabilities Affecting Cisco Products: August 2026