INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-01 14:58 UTC

Seven ClamAV Parser Flaws Enable Remote DoS in Cisco Secure Endpoint; Windows Deployments Face Elevated RCE Risk

CVE VULNERABILITY | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0377
Type	CVE Vulnerability
CVE ID	CVE-2026-20213, CVE-2026-20214, CVE-2026-20215, CVE-2026-20216, CVE-2026-20217, CVE-2026-20243, CVE-2026-20244
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Cisco Secure Endpoint Connector for Windows, Linux, and macOS; Cisco Secure Endpoint Private Cloud (connector software only)
Published	2026-07-01T16:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

Cisco disclosed seven vulnerabilities in ClamAV file format parsers affecting Cisco Secure Endpoint Connector for Windows, Linux, and macOS, each rated CVSS 7.5. An unauthenticated remote attacker can submit a specially crafted file to crash the scanning engine, disabling endpoint protection across affected deployments. Windows deployments carry the highest risk; Cisco's advisory notes that analogous memory corruption classes have historically led to remote code execution on 32-bit Windows, though no active exploitation has been confirmed as of the advisory date.

Technical Analysis

Cisco PSIRT disclosed seven ClamAV parser vulnerabilities: CVE-2026-20213, CVE-2026-20214, CVE-2026-20215, CVE-2026-20216, CVE-2026-20217, CVE-2026-20243, and CVE-2026-20244. All carry CVSS 7.5. Affected products include Cisco Secure Endpoint Connector for Windows, Linux, and macOS, and the connector software component of Cisco Secure Endpoint Private Cloud. CWE classifications span three distinct weakness classes: buffer overflow (CWE-120), uncontrolled resource consumption (CWE-770), and integer overflow (CWE-190), indicating the flaws reside across multiple independent parser code paths rather than a single shared component. Attack vector is network-based and unauthenticated: an attacker submits a specially crafted file that triggers the vulnerable parser, causing a denial-of-service condition. Windows

deployments carry elevated risk because ClamAV runs in a privileged context on that platform; Cisco's advisory notes that analogous memory corruption classes have historically led to remote code execution on 32-bit Windows. MITRE technique mapping includes T1499.004 (Application or System Exploitation for resource exhaustion), T1203 (Exploitation for Client Execution), T1562.001 (Impair Defenses: Disable or Modify Tools), T1105 (Ingress Tool Transfer), and T1499 (Endpoint Denial of Service). No active exploitation has been confirmed as of the advisory date. Patches are available from Cisco. Source: Cisco PSIRT advisory. Note: the NVD source entry in the pipeline references CVE-2026-26794, which does not correspond to any of the seven CVEs in this advisory; no claims in this report are drawn from that source.

Action Checklist

1. Step 1: Containment. Identify all hosts running Cisco Secure Endpoint Connector for Windows, Linux, or macOS, and all Cisco Secure Endpoint Private Cloud deployments using the connector software. Prioritize 32-bit Windows hosts, which Cisco's advisory identifies as carrying the highest exposure. Verify patch availability against the Cisco PSIRT advisory at https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyxR. Isolate or restrict file submission paths to unpatched connectors where operationally feasible. (CIS 1.1, Establish and Maintain Detailed Enterprise Asset Inventory; CIS 2.2, Ensure Authorized Software is Currently Supported)
2. Step 2: Detection. Query endpoint management consoles and EDR telemetry for Cisco Secure Endpoint Connector version strings to confirm which hosts are running vulnerable builds. Review ClamAV scan daemon logs for unexpected process crashes, scan engine restarts, or abnormal memory consumption patterns correlated with file scan events. Monitor for MITRE T1562.001 indicators: unexpected termination or disabling of the ClamAV scanning process. Check for repeated submission of the same crafted file type from external or internal sources (T1499.004). (NIST AU-6, Audit Record Review, Analysis, and Reporting; NIST AU-2, Event Logging; CIS 8.2, Collect Audit Logs)
3. Step 3: Eradication. Apply the patched ClamAV version provided in the Cisco PSIRT advisory (https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyxR) to all affected Connector deployments. Follow Cisco's documented upgrade path for Cisco Secure Endpoint Private Cloud connector components. Do not rely on network-layer filtering alone as a substitute for patching; the attack surface is the file scanning function itself. (CIS 7.3, Perform Automated Operating System Patch Management; CIS 7.4, Perform Automated Application Patch Management; NIST CM-6, Configuration Settings)
4. Step 4: Recovery. After patching, confirm the ClamAV scanning process starts cleanly and processes a representative file set without error. Validate that no scan engine crashes or anomalous restarts appear in post-patch logs. Re-enable any file submission paths that were restricted during containment. Verify connector version strings in your endpoint management console match the patched build. (NIST CP-10, System Recovery and Reconstitution; NIST AU-3, Content of Audit Records)
5. Step 5: Post-Incident. Review asset inventory completeness for endpoint security tooling to confirm all Connector deployments were identified promptly (gap: CIS 1.1). Assess whether patch deployment timelines for endpoint security agent software meet your vulnerability remediation SLA (CIS 7.2, Establish and Maintain a Remediation Process). Evaluate whether ClamAV process crashes on production endpoints generate alerts in your SIEM, and tune alerting if not (NIST AU-5, Response to Audit Logging Process Failures). Document whether 32-bit Windows Connector deployments are still in active use and initiate a migration plan if so, given the elevated historical RCE precedent noted in Cisco's advisory.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal/compliance if ClamAV crash logs on any 32-bit Windows Connector host correlate with an external inbound file submission and are followed by anomalous outbound connections or new process creation from the clamd.exe parent — this pattern is consistent with RCE exploitation and triggers breach notification assessment under applicable data protection regulations.
Recovery Notes	After patching all Connector deployments, monitor ClamAV daemon logs and Windows Application Event Log (Source: CiscoAMP) continuously for at least 72 hours for any recurrence of process crashes or scan engine restarts, as a crafted file already resident in a monitored file share or email queue could re-trigger the vulnerability if scan jobs are queued. Re-validate connector version strings in the endpoint management console against the Cisco PSIRT advisory's minimum safe build number for all three platforms (Windows, Linux, macOS) before closing the incident. Confirm that Cisco Secure Endpoint Private Cloud connector components were upgraded via Cisco's documented Private Cloud upgrade path, as these components do not update through the same channel as standard connector deployments.
Forensic Artifacts	ClamAV daemon crash logs at /var/log/clamav/clamd.log (Linux/macOS) or %ProgramData%\Cisco\AMP\log\sfc.exe.log (Windows) — parser-specific 'LibClamAV Error' or 'Assertion failed' entries identify which of the seven CVE-affected file format parsers was triggered and the filename or scan path that caused the crash | Windows Application Event Log entries with Source 'CiscoAMP', Event IDs 1000 (Application Error) or 1001 (Application Hang) referencing clamd.exe or sfc.exe, with faulting module path pointing to the ClamAV parser DLL — correlate timestamps with inbound file delivery events to establish exploitation timeline | Crafted trigger files retained in ClamAV scan queue or temp directories (%TEMP%\clamav-* on Windows; /tmp/clamav-* on Linux) at the time of crash — these files are the weaponized inputs and should be preserved as evidence and submitted to Cisco PSIRT and sandbox analysis | Network flow logs (NetFlow, firewall, or proxy logs) capturing the source IP, protocol, and file transfer session that preceded each clamd crash event — critical for distinguishing targeted delivery of a crafted file from opportunistic web/email scanning activity, and for identifying whether the same source triggered crashes on multiple hosts | Memory dump of the clamd.exe or clamd process captured immediately after crash (Windows Error Reporting %LOCALAPPDATA%\CrashDumps\clamd.exe.*.dmp or Linux core dump) — enables analysis of heap state at time of fault to determine whether memory corruption progressed beyond DoS toward code execution, specifically relevant for 32-bit Windows Connector hosts where Cisco's advisory flags historical RCE precedent

Per-Action IR Details

Step 1: Containment — Identify all hosts running Cisco Secure Endpoint Connector for Windows, Linux, or macOS, and all Cisco Secure Endpoint Private Cloud deployments using the connector software. Prioritize 32-bit Windows hosts, which Cisco's advisory identifies as carrying the highest exposure. Verify patch availability against the Cisco PSIRT advisory at https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyxR. Isolate or restrict file submission paths to unpatched connectors where operationally feasible. (CIS 1.1 — Establish and Maintain Detailed Enterprise Asset Inventory; CIS 2.2 — Ensure Authorized Software is Currently Supported)

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), NIST CM-8 (System Component Inventory)

Compensating: Run 'Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -like "*Secure Endpoint*"}' across Windows hosts via PowerShell remoting to enumerate connector versions. On Linux/macOS, use 'ssh -i key user@host dpkg -l | grep amp' or equivalent osquery query: 'SELECT name, version FROM programs WHERE name LIKE "%Secure Endpoint%";'. Block external file relay paths (email attachments, web upload endpoints) at the perimeter firewall for unpatched 32-bit Windows hosts using iptables or Windows Firewall rules until patching is complete.

Evidence: Before restricting file submission paths or isolating any host, capture: (1) current ClamAV clamd process memory via 'procdump -ma clamd.exe' (Windows) or 'gcore $(pgrep clamd)' (Linux) to preserve any in-memory indicators of prior exploitation attempts; (2) active network connections to the connector with 'Get-NetTCPConnection | Where-Object {$_.OwningProcess -eq (Get-Process clamd).Id}' or 'ss -tpn | grep clamd'; (3) connector version registry key at HKLM\SOFTWARE\Cisco\AMP\VersionInfo (Windows) or /opt/cisco/amp/bin/ampdaemon --version output. These volatile states are destroyed upon host isolation or service restart.

Step 2: Detection — Query endpoint management consoles and EDR telemetry for Cisco Secure Endpoint Connector version strings to confirm which hosts are running vulnerable builds. Review ClamAV scan daemon logs for unexpected process crashes, scan engine restarts, or abnormal memory consumption patterns correlated with file scan events. Monitor for MITRE T1562.001 indicators: unexpected termination or disabling of the ClamAV scanning process. Check for repeated submission of the same crafted file type from external or internal sources (T1499.004). (NIST AU-6 — Audit Record Review, Analysis, and Reporting; NIST AU-2 — Event Logging; CIS 8.2 — Collect Audit Logs)

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: On Windows, query Sysmon Event ID 1 (Process Create) and Event ID 5 (Process Terminate) filtering on 'clamd.exe' or 'freshclam.exe' to detect unexpected restarts: 'Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational | Where-Object {$_.Id -eq 5 -and $_.Message -like "*clamd*"}'. On Linux, run 'journalctl -u clamd -p err --since "24 hours ago"' or parse /var/log/clamav/clamd.log for 'Aborted', 'Segmentation fault', or 'ERROR' strings. Use osquery: 'SELECT * FROM process_events WHERE name="clamd" AND cmdline LIKE "%crash%";' to correlate crash events with inbound file scan requests from specific source IPs.

Evidence: Before any remediation action, preserve: (1) ClamAV daemon log at /var/log/clamav/clamd.log (Linux/macOS) or %ProgramData%\Cisco\AMP\log\sfc.exe.log (Windows) — look for 'LibClamAV Error', 'Assertion failed', or heap corruption messages tied to specific file format parser names (matching the seven CVE-affected parsers); (2) Windows Application Event Log entries with Source 'CiscoAMP' or 'clamd' around crash timestamps (Event IDs 1000/1001 for application faults); (3) copies of any file objects present in the ClamAV scan queue or temp directory at time of crash (typically %TEMP%\clamav-* or /tmp/clamav-*) — these may be the crafted trigger files; (4) network flow logs showing the source IP and file transfer protocol used to deliver the file that preceded each crash event.

Step 3: Eradication — Apply the patched ClamAV version provided in the Cisco PSIRT advisory (cisco-sa-clamav-88cFYyxR) to all affected Connector deployments. Follow Cisco's documented upgrade path for Cisco Secure Endpoint Private Cloud connector components. Do not rely on network-layer filtering alone as a substitute for patching — the attack surface is the file scanning function itself. (CIS 7.3 — Perform Automated Operating System Patch Management; CIS 7.4 — Perform Automated Application Patch Management; NIST CM-6 — Configuration Settings)

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), NIST CM-6 (Configuration Settings), NIST SI-2 (Flaw Remediation)

Compensating: For teams without enterprise patch management, download the patched Cisco Secure Endpoint Connector installer directly from the Cisco PSIRT advisory page and deploy via PowerShell remoting: 'Invoke-Command -ComputerName $hostList -ScriptBlock {Start-Process msiexec.exe -ArgumentList "/i C:\temp\amp_connector_patched.msi /quiet" -Wait}'. On Linux, distribute via SSH with 'scp amp_connector_patched.rpm user@host:/tmp/ && ssh user@host "sudo rpm -Uvh /tmp/amp_connector_patched.rpm"'. Verify patched version with 'Get-ItemProperty HKLM:\SOFTWARE\Cisco\AMP\VersionInfo' post-install. Prioritize 32-bit Windows hosts first given Cisco's elevated RCE precedent note.

Evidence: Before applying the patch and restarting the ClamAV/clamd service — which will destroy live process state — capture: (1) full memory dump of the running clamd process ('procdump -ma clamd.exe' on Windows; 'gcore $(pgrep clamd)' on Linux) to enable post-hoc analysis of any heap corruption or shellcode if exploitation is suspected; (2) a snapshot of all files currently staged in the ClamAV scan queue or temp directory (%TEMP%\clamav-* or /tmp/clamav-*) as potential crafted trigger artifacts; (3) current connector version string from registry or filesystem before overwrite by the installer, to document the vulnerable build in your incident record.

Step 4: Recovery — After patching, confirm the ClamAV scanning process starts cleanly and processes a representative file set without error. Validate that no scan engine crashes or anomalous restarts appear in post-patch logs. Re-enable any file submission paths that were restricted during containment. Verify connector version strings in your endpoint management console match the patched build. (NIST CP-10 — System Recovery and Reconstitution; NIST AU-3 — Content of Audit Records)

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST CP-10 (System Recovery and Reconstitution), NIST AU-3 (Content of Audit Records), NIST CM-6 (Configuration Settings)

Compensating: Submit a controlled set of benign test files of each format type affected by the seven CVEs (confirm format list from Cisco advisory) to the patched connector using ClamAV's 'clamdscan --fdpass /path/to/testfiles/' and verify zero crashes and clean exit codes. On Windows, monitor Sysmon Event ID 5 for clamd.exe process termination events for 24 hours post-patch. Run 'Get-EventLog -LogName Application -Source CiscoAMP -Newest 50' to confirm absence of post-patch fault entries. Document patched version string from 'HKLM:\SOFTWARE\Cisco\AMP\VersionInfo' and compare against advisory's minimum safe build number.

Evidence: This step re-enables file submission paths (alters network/service state) — before doing so, confirm post-patch log baseline is clean: review /var/log/clamav/clamd.log or Windows %ProgramData%\Cisco\AMP\log\sfc.exe.log for the 30-minute window immediately following service restart to establish a crash-free baseline. Retain pre-patch and post-patch connector version registry snapshots and log excerpts as documentary evidence for change control records and any subsequent audit under NIST AU-3.

Step 5: Post-Incident — Review asset inventory completeness for endpoint security tooling to confirm all Connector deployments were identified promptly (gap: CIS 1.1). Assess whether patch deployment timelines for endpoint security agent software meet your vulnerability remediation SLA (CIS 7.2 — Establish and Maintain a Remediation Process). Evaluate whether ClamAV process crashes on production endpoints generate alerts in your SIEM, and tune alerting if not (NIST AU-5 — Response to Audit Logging Process Failures). Document whether 32-bit Windows Connector deployments are still in active use and initiate a migration plan if so, given the elevated historical RCE precedent noted in Cisco's advisory.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), NIST AU-5 (Response

to Audit Logging Process Failures), NIST CM-8 (System Component Inventory)

Compensating: Use osquery scheduled query 'SELECT name, version, install_location FROM programs WHERE name LIKE "%Secure Endpoint%" OR name LIKE "%ClamAV%";' deployed as a persistent pack across all endpoints to maintain a live connector version inventory that auto-detects future vulnerable builds. Write a Sigma rule targeting Windows Application Event Log Source='CiscoAMP' EventID=1000/1001 (application crash) to generate SIEM or local alert on any future clamd.exe fault. Archive the 32-bit Windows host list produced during this incident as a tracked remediation item with a target migration date.

Evidence: No live-state altering actions occur in this phase, so no volatile capture prerequisite applies. Preserve as post-incident documentation: (1) the full list of affected hosts by OS and connector version enumerated during Step 1, with timestamps of patch application per host; (2) any clamd crash log excerpts collected during Steps 2-3 that correlated with external file submissions, as evidence of exploitation attempts vs. incidental crashes; (3) the delta between initial asset inventory and actual hosts discovered during response, to quantify the CIS 1.1 coverage gap for the lessons-learned report.

Detection Guidance

Query your endpoint management platform or EDR for installed Cisco Secure Endpoint Connector version strings across all Windows, Linux, and macOS assets to identify unpatched hosts. In ClamAV scan daemon logs, look for unexpected clamd process terminations, scan engine restart events, or out-of-memory kills correlated with file scan activity - these are the expected crash signatures for the DoS condition. In SIEM, build a detection rule for repeated scan failures or clamd restarts within a short time window from the same source, which may indicate active exploitation attempts (T1499.004). Monitor for T1562.001 indicators: any event showing the ClamAV or Cisco Secure Endpoint scanning process stopping unexpectedly without an administrative trigger. On Windows, check Windows Event Logs for application crashes (Event ID 1000) attributed to the Cisco Secure Endpoint or ClamAV process. No public IOCs (IPs, domains, file hashes) have been released as of the advisory date, consistent with no confirmed active exploitation. (NIST AU-6; NIST AU-2; CIS 8.2)

Framework Mappings

MITRE-ATTACK

- **T1203** — Exploitation for Client Execution
- **T1499.004** — Application or System Exploitation
- **T1105** — Ingress Tool Transfer
- **T1499** — Endpoint Denial of Service
- **T1562.001** — Disable or Modify Tools

NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring
- **SC-5** — Denial-of-Service Protection

- **SI-16** — Memory Protection
- **AT-2** — Literacy Training and Awareness
- **IR-5** — Incident Monitoring

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

OWASP-TOP10-2021

- **A03:2021** — Injection

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1203	Exploitation for Client Execution	Execution
T1499.004	Application or System Exploitation	Impact
T1105	Ingress Tool Transfer	Command-And-Control
T1499	Endpoint Denial of Service	Impact
T1562.001	Disable or Modify Tools	Defense-Evasion

Sources

Source	URL	Tier
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T1
Networkworld	https://www.networkworld.com/article/3523958/cisco-latest-news-and-...	T3
SecurityWeek	https://www.securityweek.com/cisco-patches-critical-vulnerabilities...	T2
Talosintelligence	https://blog.talosintelligence.com/toolshell-affecting-sharepoint-s...	T1

Source	URL	Tier
CVE-2026-26794 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2026-26794	**T1**
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	**T1**

Generated 2026-07-01 14:58 UTC by TJS Security Command Center