

SECURITY ADVISORY

Cisco Secure Email Gateway Critical File Write and RCE

An actively exploited email-processing vulnerability can give unauthenticated attackers root-level command execution.

SEVERITY	PUBLISHED	CATEGORY	STATUS
CRITICAL	14 OCT 2026	EMAIL / RCE	PATCH AVAILABLE

Reviewed 23 Oct 2026. Severity and scope details appear below.

Severity: CRITICAL · Category: Email Security / RCE · Status: Patch available; exploitation reported. CVE-2026-76519 is rated CVSS v3.1 9.8. Published 14 October 2026; reviewed 23 October 2026.

URGENT ACTION

Confirm the scanner update or fixed AsyncOS release is installed on every affected gateway. Cisco reports active exploitation and no workaround. Investigate exposed appliances, including every cluster member, before assuming patching has restored trust. [1, 2]

01 INCIDENT SUMMARY

Cisco disclosed CVE-2026-76519 on 14 October 2026. Improper attachment handling in the Advanced Malware Protection (AMP) feature can permit unauthenticated arbitrary file writes and root-level command execution. Exploitation involves a crafted email passing through a vulnerable gateway. [1, 2]

Exposure requires a vulnerable AsyncOS release, File Reputation enabled in a mail policy, and Content Scanner Tools below 25.3.0.5525. Both physical and virtual Secure Email Gateway appliances can be affected. [1]

02 POTENTIAL IMPACT

- Appliance compromise: Arbitrary file writes can lead to commands running with root privileges. [1, 2]
- Cluster exposure: Stolen inter-appliance SSH keys may permit access to additional cluster members. [2]
- Reduced forensic visibility: An attacker with root access may hide or remove evidence; a clean local log result does not conclusively exclude compromise. [1, 2]

03 PRIORITY ACTIONS FOR CUSTOMERS

1. Confirm configuration and ownership

Inventory gateways and clusters. Record the AsyncOS release, scanner package and File Reputation policy state. Include externally managed appliances and identify the responsible provider.

2. Apply and verify the fix

Check Content Scanner Tools with contentscannerstatus. Where required, use contentscannerupdate or the supported fixed AsyncOS release. The scanner update requires neither an AsyncOS upgrade nor a restart; verify its installation rather than assuming automatic updates succeeded. [1]

3. Investigate each cluster member

Review System Security entries in system_logs and correlate findings with independent firewall and network logs. Preserve evidence and contact Cisco TAC for suspected compromise or an incomplete security scan. [2]

4. Recover compromised appliances safely

Follow Cisco's platform-specific recovery guidance. For virtual appliances, preserve evidence before rebuilding, avoid importing an untrusted configuration and renew exposed credentials and cryptographic material. Assess all members of a compromised cluster. [1]

TECHNICAL & RESPONSE DETAILS

Guidance for infrastructure, development, operations and security teams

04 TECHNICAL INFORMATION

- Identifier / weakness: CVE-2026-76519; relative path traversal in AMP attachment processing. [2]
- Severity / access: Critical, CVSS v3.1 9.8; no attacker login required under the affected configuration. [1, 2]
- Exploitation status: Cisco PSIRT reports active exploitation in October 2026. [1]
- Detection focus: Local security-scan messages, unexpected outbound traffic and suspicious appliance changes; corroborate results with external telemetry. [2]

05 PATCHED VERSIONS AND EXPOSURE

- Content Scanner Tools: 25.3.0.5525 or later includes the fix on licensed, supported AsyncOS releases.
- AsyncOS 15.5: fixed in 15.5.5-014. AsyncOS 16.5: fixed in 16.5.0-780. AsyncOS 16.0: migrate to a fixed release. [1, 2]
- Cisco Secure Email Cloud Gateway: Cisco has deployed the scanner fix; follow any separate customer-specific recovery notification.
- Secure Email and Web Manager and Secure Web Appliance: Cisco lists these products as not affected by this vulnerability. [1, 2]

06 VALIDATION CHECKLIST

- Verify the fixed scanner version or AsyncOS build on every in-scope appliance.
- Test mail flow, quarantine handling and expected malware-policy enforcement.
- Retain external logs and document compromise-assessment findings for each cluster member.
- Restrict management access and track recovery, credential renewal and provider actions.

ADVISORY BASIS

Independent 443 Labs customer awareness guidance. Publication date follows Cisco's 14 October disclosure; sources were reviewed on 23 October 2026. Applicability depends on the deployed configuration. This advisory does not establish compromise of any recipient.

PRIMARY SOURCES

[1] [Cisco security advisory cisco-sa-esa-afw-zqYJkxp - 14 October 2026](#)

[2] [CERT-EU advisory 2026-017 - 15 October 2026](#)