Critical Cisco Secure Email Gateway flaw under active exploitation



CERT-EU reports that CVE-2026-76519 (CVSS 9.8) in Cisco Secure Email Gateway lets an unauthenticated attacker run commands as root, and Cisco is aware of active exploitation. Update and check appliances for compromise.

- CVE-2026-76519 has a CVSS score of 9.8 and affects the Advanced Malware Protection feature.
- An unauthenticated remote attacker could write files and execute commands as root using a crafted email attachment.
- Cisco PSIRT is aware of active exploitation.
- Exposure requires File Reputation enabled in a mail policy and Content Scanner Tools earlier than 25.3.0.5525.
- Compromised appliances may expose SSH keys used between cluster members.

On 14 October 2026 Cisco published an advisory on a critical flaw in the Advanced Malware Protection (AMP) feature of Cisco Secure Email Gateway. CERT-EU relayed it the next day, noting that Cisco PSIRT is aware of active exploitation.

What the flaw allows

CVE-2026-76519 (CVSS 9.8) is a relative path traversal issue caused by improper handling of email attachments when the file reputation service is enabled. An attacker sends an email with a crafted attachment through a vulnerable device and may then write arbitrary files and run commands with root privileges, with no authentication.

Cisco notes that appliances may sit in clusters. On a compromised appliance, the private SSH keys used between cluster members could be reached, which may let the attacker compromise other members. Attackers may also remove or hide evidence of exploitation.

Who is affected

Physical and virtual appliances running AsyncOS 15.5 before 15.5.5-014, 16.0, or 16.5 before 16.5.0-780 are affected, provided File Reputation is enabled and assigned to a mail policy and Content Scanner Tools is earlier than 25.3.0.5525. Secure Email and Web Manager and Secure Web Appliance are not affected. Secure Email Cloud Gateway customers need take no action, as the fixed package is already deployed.

Recommended response

CERT-EU urges updating Content Scanner Tools or upgrading AsyncOS as soon as possible, starting with internet-reachable appliances. Cisco advises reviewing system logs on each device for compromise messages. Because root access lets attackers hide traces, it also advises cross-checking network and firewall logs outside the device for unexpected uploads to external IP addresses or downloads from malicious ones. Cisco has published no specific indicators of compromise.

What to do now

1. Inventory all Cisco Secure Email Gateway appliances, including cluster members, and check AsyncOS and Content Scanner Tools versions.
2. Confirm whether File Reputation is enabled and assigned to any mail policy.
3. Update Content Scanner Tools to 25.3.0.5525 or later, or upgrade AsyncOS to a fixed release, starting with internet-reachable appliances.
4. Review system logs on each appliance for the compromise messages Cisco describes, and trigger incident response if one is found.
5. Cross-check network and firewall logs for unexpected uploads to external IPs or downloads from malicious IPs.

6. If compromise is detected or suspected, assess other cluster members and contact Cisco TAC.