



Security Advisory 2026-017

Critical Vulnerability in Cisco Secure Email Gateway

2026-10-15 — v1.0

TLP:CLEAR

History:

- 15/10/2026 — v1.0 – Initial publication

Summary

On 14 October 2026, Cisco published a security advisory addressing a **critical vulnerability** affecting the **Advanced Malware Protection (AMP) feature of Cisco Secure Email Gateway**. This vulnerability could allow an unauthenticated, remote attacker to write arbitrary files and execute commands with root privileges on the underlying operating system [1].

The Cisco PSIRT is aware of **active exploitation** of this vulnerability [1].

CERT-EU strongly recommends updating the Content Scanner Tools package or upgrading Cisco AsyncOS Software to a fixed release as soon as possible, prioritising appliances reachable from the internet. CERT-EU also recommends checking all affected appliances for indicators of compromise.

Technical Details

The vulnerability **CVE-2026-76519**, with a CVSS score of 9.8, is a **relative path traversal** flaw in the AMP feature of Cisco Secure Email Gateway that allows an **unauthenticated, remote attacker to write arbitrary files on the underlying operating system**. The vulnerability is due to **improper handling of email attachments** when the file reputation service is enabled. An attacker could exploit it by sending an email that contains a crafted attachment through an affected device, and a successful exploit could allow the attacker to write arbitrary files and execute commands with root privileges [1].

Cisco notes that Secure Email Gateway appliances can be part of clusters, and that private SSH keys used for authentication between cluster members could be accessed on a compromised appliance, which may allow the attacker to compromise other cluster members. Upon successful exploitation, attackers may also remove or hide evidence of exploitation and indicators of compromise [1].

Affected Products

The vulnerability affects **Cisco Secure Email Gateway** (both physical and virtual) running the following versions of **Cisco AsyncOS Software** [1]:

- versions 15.5 before 15.5.5-014
- versions 16.0
- versions 16.5 before 16.5.0-780

The following conditions **should also be met** [1]:

- The File Reputation service, which is part of Cisco AMP, is enabled and assigned to a mail policy.
- The Content Scanner Tools version is earlier than 25.3.0.5525.

The information above reflects Cisco's fixed release information. The fix is also distributed to all licensed and supported Cisco AsyncOS Software releases through an updated Content Scanner Tools package, and Content Scanner Tools versions 25.3.0.5525 and later contain the fix [1].

To determine whether the File Reputation service is enabled, administrators can choose **Mail Policies > Incoming Mail Policies > Advanced Malware Protection** or **Mail Policies > Outgoing Mail Policies > Advanced Malware Protection** in the web-based management interface, select a mail policy, and inspect the **Enable File Reputation** check box. To determine the running Content Scanner Tools version, Cisco provides the following CLI command [1]:

```
contentsscannerstatus
```

Cisco has confirmed that this vulnerability **does not affect Secure Email and Web Manager or Secure Web Appliance**. For Cisco Secure Email Cloud Gateway customers, Cisco states that no action is required, as a fixed version of Content Scanner Tools is already deployed [1].

Additional information is available in the vendor's advisory [1].

Recommendations

CERT-EU strongly recommends updating the Content Scanner Tools package or upgrading Cisco AsyncOS Software to a fixed release as soon as possible, prioritising appliances reachable from the internet. CERT-EU also recommends checking all affected appliances for indicators of compromise.

Compromise assessment

Cisco recommends reviewing the system logs for each affected device, with the following command, to identify exploitation attempts [1]:

```
grep "System Security" system_logs
```

One of the log messages in the following table may be in the output [1]:

Log message	Recommended action
System Security: Suspected compromise indicator was found. Contact TAC for further recommendations.	A compromise is detected. Trigger the incident response plan.

Log message	Recommended action
System Security: Security scan did not complete. Contact TAC for further recommendations.	A compromise is suspected. Trigger the incident response plan, and contact the Cisco Technical Assistance Center (TAC) for further support.
System Security: No compromise indicator was found.	No compromise detected.

Vendor's note: Upon successful exploitation of this vulnerability, attackers may obtain command execution with root privileges. With this level of access, attackers may remove or hide evidence of exploitation and indicators of compromise. Cisco strongly recommends cross-checking the network logs and the firewall logs outside of the impacted device to identify any potential suspicious activity, including but not limited to unexpected uploads that were initiated from the affected device to external IP addresses or downloads from malicious IP addresses.

In their advisory, Cisco does not mention any actual Indicator of Compromise. It is also not known how the log messages described above are generated.

References

- [1] <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkjpg>