

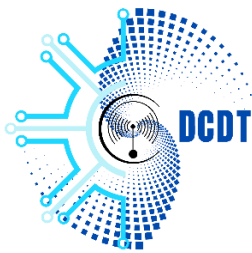
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

15 October 2026

Advisory 357: Cisco Secure Email Gateway Path Traversal Remote Code Execution Vulnerability - Actively Exploited (CVE-2026-76519).

Release Date: 14th October 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-76519 is a critical path traversal vulnerability (relative path traversal) in the Advanced Malware Protection feature of Cisco Secure Email Gateway. An unauthenticated remote attacker can send an email with a crafted attachment to write files to the underlying operating system of the appliance, and a successful attack could lead to command execution as root. It is rated CVSS 9.8. Cisco found the flaw through its own internal security testing and has updated its advisory to say it is known to be actively exploited.

What are the systems affected?

Physical and virtual Cisco Secure Email Gateway appliances are affected when File Reputation is enabled in a mail policy and Content Scanner Tools is older than 25.3.0.5525, on the following AsyncOS releases:

- AsyncOS 15.5 releases before 15.5.5-014
- AsyncOS 16.5 releases before 16.5.0-780
- AsyncOS 16.0 releases, for which Cisco has no fix (migrate to a fixed release)

Not affected / patched version:

- Content Scanner Tools 25.3.0.5525 or later, which removes the vulnerable condition without an upgrade or restart
- AsyncOS 15.5.5-014 or 16.5.0-780 or later. Cisco advises gateways on releases earlier than 16.5 to move to 16.5.0-780

What does this mean?

Successful exploitation may allow attackers to:

- Write attacker-chosen files to the appliance by sending a single crafted email attachment, without credentials
- Possibly run commands as root on the email gateway, which sits in front of all inbound and outbound mail
- Read, alter or divert email, steal credentials and use the gateway as a foothold into the internal network

Mitigation process

CERTVU recommends the following:

1. Update Content Scanner Tools now

Run `contentscannerupdate` (or enable automatic updates) on every gateway and verify the version with `contentscannerstatus`. This can be done without a restart and removes the vulnerable condition.

2. Upgrade AsyncOS

Move gateways to 15.5.5-014 or 16.5.0-780 or later, and migrate any 16.0 gateway to a fixed release because it will not be patched.

3. Check every appliance for compromise

4. Respond to a confirmed compromise

5. Treat this as top priority

Reference

1. <https://thehackernews.com/2026/10/cisco-warns-of-active-attacks.html>
2. <https://www.bleepingcomputer.com/news/security/cisco-patches-actively-exploited-secure-email-gateway-zero-day/>
3. <https://sec.cloudapps.cisco.com/security/center/publicationListing.x>
4. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>