contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Cisco Secure Email Gateway exploited

CVE-2026-76519 · on CISA's exploited list since 14 October 2026

Analysis Report

If you run Cisco Secure Email Gateway with File Reputation assigned to a mail policy, act today: CISA's date has passed. First check whether Content Scanner Tools is earlier than 25.3.0.5525. If it …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	STATUS	On CISA's exploited list; due 17 October 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/cisco-secure-email-gateway-cve-2026-76519

The bottom line

> *If you run Cisco Secure Email Gateway with File Reputation assigned to a mail policy, act today: CISA's date has passed. First check whether Content Scanner Tools is earlier than 25.3.0.5525. If it is not, or you do not run the product, you can stop here.*

At a glance

Fact	Detail
Product	Cisco Secure Email Gateway (CVE-2026-76519)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 14 October 2026. Deadline for US federal agencies: 17 October 2026.
Chance of exploitation (EPSS)	0.02, the estimated chance in the next 30 days, as at 1 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	The advisory says Content Scanner Tools earlier than 25.3.0.5525 is affected. The AsyncOS fixed releases are not in the text we have.
Who looks first	Anyone running Cisco Secure Email Gateway, physical or virtual, with File Reputation (part of AMP) assigned to a mail policy and Content Scanner Tools earlier than 25.3.0.5525. Not Secure Email and Web Manager or Secure Web Appliance.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Cisco Secure Email Gateway, physical or virtual?	Nothing to do for this CVE.	Check whether File Reputation is on (next question).
Is File Reputation enabled and assigned to an incoming or outgoing mail policy?	Not affected as the advisory describes it. Recheck if that changes.	Check the Content Scanner Tools version (next question).
Is Content Scanner Tools earlier than 25.3.0.5525?	Not affected as the advisory describes it.	Update now, then check the logs (next question).

Can mail from outside your organisation reach this gateway?	Risk is lower, but still update. Attachments are the trigger, not a login.	Treat as urgent. Anyone who can send you mail can reach the flaw.

What it is

An unauthenticated attacker can send an email with a crafted attachment through the device. The record says this lets them write arbitrary files and run commands with root privileges on the underlying system. The advisory says there is no workaround.

Why it matters

Our reading is that a mail gateway sits on the path of all inbound mail. The attacker needs no account, only a message that passes through the device. Root on that system would be a strong foothold at the edge of the network. The score is 9.8, the weakness is CWE-23 (relative path traversal), and the advisory says no workaround exists. That makes updating the only real route.

What the vendor's advisory says

We read one page on sec.cloudapps.cisco.com. In short:

- The vendor's advisory was first published on 14 October 2026 and rates the flaw Critical, base score 9.8.
- The advisory says no workarounds are available, and that Cisco has released software updates.
- The advisory says Secure Email and Web Manager and Secure Web Appliance are not vulnerable.
- The advisory says to check system_logs for entries containing "System Security", on every device if the gateway is in a cluster.
- The advisory points to the Secure Email Gateway Security Hardening Release of September 2026 for fixes; the Fixed Software section is not in the text we have.

Things people will get wrong

- "We have File Reputation off on one policy, so we are fine." The advisory says it matters if the service is enabled and assigned to any mail policy, incoming or outgoing. Check every policy.
- "We can block it with a setting until we patch." The advisory says there are no workarounds that address this vulnerability.
- "The attacker needs a login or a user to open the attachment." The record says the attacker is unauthenticated and remote. The flaw is in how the device handles the attachment as mail passes through it.

The wording includes conditions the score may not show: it needs privileges. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

Step 1: Find the versions you run

- Run contentscannerstatus on the CLI and read the Content Scanner Tools version. Affected means earlier than 25.3.0.5525.
- In the web interface, open each mail policy's Advanced Malware Protection page and see whether Enable File Reputation is ticked.

Step 2: Check for signs of exploitation

- The advisory says to review system_logs for entries containing "System Security", on each cluster device.
- CISA lists this as exploited, so check before you update, and keep a copy of the logs.

Step 3: Update

- Apply the update Cisco names in its advisory. The advisory says no workaround exists.
- Ask Cisco or your provider for the exact fixed release for your AsyncOS version, as the text we have does not name one.

Step 4: Confirm the fix

- Run contentscannerstatus again and confirm the version is 25.3.0.5525 or later.
- Get the result in writing from whoever runs the gateway.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello. We need to confirm our exposure to CVE-2026-76519 in Cisco Secure Email Gateway, which CISA lists as exploited. Please tell us whether we run this product, physical or virtual, and on which devices. Please tell us whether File Reputation is enabled on any mail policy, and the Content Scanner Tools version on each device. The vendor's advisory says versions earlier than 25.3.0.5525 are affected. Please also say whether you have checked system_logs for "System Security" entries. Please confirm the fix and the version in writing by a date you propose, ideally within two working days.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Entries containing "System Security" in system_logs, on every cluster device; the advisory lists messages in a table that we could not see.
- Files on the appliance that you did not put there, since the flaw lets an attacker write arbitrary files.
- Inbound messages with unusual attachments that passed through a mail policy with File Reputation enabled.

The weakness behind it

The record classes this as CWE-23 (Relative Path Traversal).

The sources, in their words

CISA's catalogue entry:

> *Cisco Secure Email Gateway contains a relative path traversal vulnerability that could allow an unauthenticated, remote attacker to write arbitrary files on the underlying operating system.*

The CVE record, published by Cisco on 14 October 2026:

> *A vulnerability in the Advanced Malware Protection (AMP) feature of Cisco Secure Email Gateway could allow an unauthenticated, remote attacker to write arbitrary files on the underlying operating system. This vulnerability is due to improper handling of email attachments when the file reputation service is enabled. An attacker could exploit this vulnerability by sending an email that contains a crafted attachment through an affected device. A successful exploit could allow the attacker to write arbitrary files and execute commands with root privileges on the underlying operating system.*

The record lists 23 affected versions or ranges of Cisco Secure Email. The first 8 are below; the rest are in the CVE record, so check your version against the whole list.

- 14.0.0-698
- 13.5.1-277
- 13.0.0-392
- 14.2.0-620
- 13.0.5-007
- 13.5.4-038
- 14.2.1-020
- 14.3.0-032

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

What we do not know yet

- Which AsyncOS releases are fixed; the Fixed Software section is not in the text we have.
- How attackers are using the flaw; the sources do not say.
- What the "System Security" log messages mean and what to do for each; the table is not in the text we have.
- Whether exploitation leaves traces after the files are written.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-76519: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
14 October 2026	CVE record published by Cisco.
14 October 2026	CISA added it to its list of exploited vulnerabilities.
17 October 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Internet-facing gateway, File Reputation on, Content Scanner Tools earlier than 25.3.0.5525	High	Now; CISA's date has passed
Clustered gateways where only some devices are checked or updated	High	Now; check every cluster device
Gateway with File Reputation off in every mail policy	Low	Next patch cycle; recheck if policy changes

Secure Email and Web Manager or Secure Web Appliance only	None	None for this CVE

Appendix 4. Definition of done

- Every Cisco Secure Email Gateway you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-76519: https://www.cve.org/CVERecord?id=CVE-2026-76519
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/c: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkjxp