

HiveForce Labs

THREAT ADVISORY

 VULNERABILITY REPORT

CVE-2026-76519: Cisco Email Gateway Zero-Day Exploited for Root Access

Date of Publication

October 15, 2026

Admiralty Code

A1

TA Number

TA2026301

Summary

First Seen: October 2026

Affected Products: Cisco Secure Email Gateway

Impact: Cisco has confirmed that attackers are actively exploiting CVE-2026-76519, a critical flaw in the Advanced Malware Protection feature of Cisco Secure Email Gateway. The appliance mishandles email attachments when its File Reputation service is turned on, which lets an attacker who has no account and no access to the network simply send an email with a specially built attachment through the gateway. The flaw carries a CVSS score of 9.8 and affects both physical and virtual appliances, but only when File Reputation is enabled and assigned to a mail policy and the Content Scanner Tools package is older than version 25.3.0.5525. Cisco Secure Email and Web Manager and Secure Web Appliance are not affected. Cisco found the flaw through its own internal security scanning and became aware of real attacks in October 2026.

CVE

CVE	NAME	AFFECTED PRODUCT	ZER O-DAY	CISA KEV	PATCH
CVE-2026-76519	Cisco Secure Email Gateway Relative Path Traversal Vulnerability	Cisco Secure Email Gateway			

Vulnerability Details

#1

CVE-2026-76519 is a path traversal issue, classified as CWE-23, in the Advanced Malware Protection feature of Cisco Secure Email Gateway. The problem lies in how the appliance handles email attachments once the File Reputation service has been switched on and attached to a mail policy. Instead of safely confining an attachment while it is examined, the gateway can be tricked into writing data outside the location it is meant to use. That single weakness turns a routine inspection step into a way of placing attacker-controlled files on the appliance's own operating system.

#2

Exploitation requires nothing more than an email. An attacker builds an attachment designed to abuse the flawed handling, sends it through an affected gateway, and the appliance does the rest while scanning it. There is no login, no prior access, and no action needed from the person the message is addressed to, which is why the attack vector is rated as network-based with low complexity and no user interaction. Once arbitrary files can be written, the attacker can reach command execution with root privileges on the underlying system, giving them full control of the appliance.

#3

Both physical and virtual gateways are affected when they run a vulnerable Cisco AsyncOS release and meet two conditions at the same time: the File Reputation service is enabled and assigned to a mail policy, and the Content Scanner Tools package is older than version 25.3.0.5525. Administrators can confirm the first by checking the Enable File Reputation box under the Advanced Malware Protection settings of an incoming or outgoing mail policy, and the second by running the `contentscannerstatus` command at the command line. Cisco has stated that Secure Email and Web Manager and Secure Web Appliance are not vulnerable, and there are no workarounds available for the appliances.

#4

Cisco discovered the issue during internal security scanning and became aware of active exploitation in October 2026, with both Cisco and the US government indicating that attacks were already under way before a fix for this specific flaw was issued. Cisco has not said how many devices were attacked or who is behind the activity, and it has directly contacted Secure Email Cloud customers where indicators of possible compromise were found.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-76519	Cisco Secure Email Gateway (AsyncOS 15.5 before 15.5.5-014, 16.0 all releases, 16.5 before 16.5.0-780; Content Scanner Tools before 25.3.0.5525)	cpe:2.3:a:cisco:secure_email_gateway:*.~.*.*.*.*.*.*	CWE-23

Recommendations



Apply the Content Scanner Tools Update First: The fastest route to safety is the Content Scanner Tools package, version 25.3.0.5525 or later, which carries the fix and installs without a software upgrade or a restart. Appliances with automatic updates enabled should already have it, but confirm it with the `contentscannerstatus` command rather than assuming it arrived. Where automatic updates are switched off, run `contentscannerupdate` at the command line, or turn automatic updates back on under Security Services > Service Updates.



Upgrade AsyncOS to a Fixed Release: Move Release 15.5 appliances to 15.5.5-014 and Release 16.5 appliances to 16.5.0-780. Release 16.0 has no fixed build, so those gateways must be migrated, and Cisco strongly recommends that anything earlier than 16.5 move to 16.5.0-780. There are no workarounds for this flaw, so an upgrade or the scanner update is the only real remediation.



Check Every Appliance for Signs of Compromise: Run `grep "System Security" system_logs` on the appliance to see whether Cisco's own security scan found anything. A suspected compromise message means the device needs incident response and a call to Cisco TAC, while an incomplete scan message also warrants TAC support. Run this on every member of a cluster, not just one, because a single unchecked device can hide the whole problem.



Do Not Trust a Clean Result on Its Own: An attacker with root can remove or disguise the evidence of their own activity, so a message saying no compromise indicator was found is reassuring but not conclusive. Cross-check firewall and network logs held outside the appliance for unusual outbound uploads from the gateway to external addresses or downloads from suspicious ones. Evidence kept somewhere the attacker could not reach is worth far more than the device's own account of itself.



Rebuild a Compromised Appliance Rather Than Upgrading It: If a virtual appliance shows signs of compromise, preserve the forensic data before doing anything else, because upgrading a compromised instance destroys the logs and evidence an investigation would depend on. Then deploy a fresh virtual machine on a fixed release, rebuild the configuration from scratch without importing any earlier configuration file, renew every credential and piece of cryptographic material, and keep monitoring the system afterwards. For a physical appliance, contact Cisco TAC and enable remote access so their engineers can investigate.



Treat the Whole Cluster as Exposed: Cluster members authenticate to each other using SSH key pairs, and those private keys could be read on a compromised appliance. That gives an attacker a credible path from one device to the rest, so Cisco recommends restoring every member of a cluster that contains at least one compromised appliance. Rotating the keys and credentials across the cluster should be part of the recovery, not an afterthought.



Harden and Restrict Access to the Appliance: Block access to the gateway from the internet wherever possible, and where it is genuinely needed, limit it to known and trusted hosts on documented ports and protocols. Separate mail traffic from management traffic onto different network interfaces, place the appliances behind a filtering device, disable HTTP for the administrator portal, and turn off any service that is not in use. Strong authentication such as SAML or LDAP and individual operator accounts in place of a shared administrator login reduce the damage if credentials ever leak.



Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities



Patch Link

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-esa-afw-zqYJkixp>



References

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-esa-afw-zqYJkixp>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of HivePro.

REPORT GENERATED ON

October 15, 2026 • 07:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com