Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Root Delivered by Email: Cisco Secure Email Gateway Zero-Day

Date of Publication	Admiralty Code	TA Number
September 16, 2026	A1	TA2026269

Summary

First Seen: September 2026
Affected Products: Cisco Secure Email Gateway (AsyncOS Software)
Impact: Cisco has disclosed CVE-2026-76461, a critical flaw in the email-parsing part of the AsyncOS software that powers Cisco Secure Email Gateway (the product once sold as the IronPort Email Security Appliance). Because this appliance scans all the mail flowing in and out of an organization, it is open to email from anyone on the internet, and the bug lets an attacker abuse that with no login, no password, and no user click required: by sending a single specially crafted email that hides SQL commands inside it, an attacker can get those commands to run on the device and escalate to full control with root privileges, effectively taking over a security appliance that was meant to protect the network. No attacker has been named yet, but the attack is easy to pull off, and the payoff is high. Cisco's related Secure Email and Web Manager and Secure Web Appliance products are not affected, and because there are no workarounds, updating to Cisco's fixed software is the only real protection.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-76461	Cisco Secure Email Gateway SQL Injection Vulnerability	Cisco Secure Email Gateway (AsyncOS)	✓	✓	✓

Vulnerability Details

#1

CVE-2026-76461 is a SQL injection weakness (CWE-89) in the email-parsing component of Cisco AsyncOS Software for Secure Email Gateway. The root cause is insufficient validation of the content the appliance handles while parsing an incoming message: SQL statements embedded in the email are passed into a database query instead of being treated as untrusted text. Because email handling is the appliance's core function and requires no sender authentication, any unauthenticated party can reach the flaw by sending a message to the device.

#2

The exploitation path is what turns a data-layer bug into full system compromise. After the malicious SQL is injected, it can be used to run arbitrary SQL and then break out into operating-system command execution with root privileges on the underlying platform. Cisco's own detection guidance highlights database "COPY .. TO PROGRAM" style behavior appearing in the mail logs, which is the mechanism by which a database statement can spawn an OS-level command. The end state is unauthenticated, remote, root-level control of the appliance.

#3

The vulnerability carries a CVSS 3.1 base score of 9.8 (Critical). It affects Cisco Secure Email Gateway in both physical and virtual form regardless of how the device is configured, while Secure Email and Web Manager and Secure Web Appliance are confirmed unaffected. The affected software spans AsyncOS 15.5 and earlier, the 16.0 train, and the 16.5 train, up to the fixed builds listed below.

#4

Active exploitation is confirmed rather than theoretical. Cisco's PSIRT became aware of attacks in September 2026; the flaw was uncovered during a Cisco TAC support case, and CISA added it to the KEV catalog the same day it was published, a strong signal that it was exploited as a zero-day before disclosure.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-76461	Cisco Secure Email Gateway (AsyncOS): 15.5 and earlier (before 15.5.5-014), 16.0 (before 16.0.4-302), 16.5 (before 16.5.0-780)	cpe:2.3:o:cisco:asyncos:*:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:secure_email_gateway_virtual_appliance:*:*:*:*:*:*:*:*:* cpe:2.3:h:cisco:secure_email_gateway:*:*:*:*:*:*:*:*:*	CWE-89

Recommendations

Patch on an Emergency Basis: Treat this as an out-of-cycle emergency update rather than routine maintenance. Upgrade Cisco Secure Email Gateway to a fixed AsyncOS build immediately: 15.5.5-014 for 15.5 and earlier, 16.0.4-302 for the 16.0 train, and 16.5.0-780 for the 16.5 train. Where possible, migrate to Cisco's recommended target release, 16.5.0-780. There are no workarounds, so patching is the only reliable protection.

Hunt for Signs of Compromise: Review the mail_logs on every gateway, and on each device in a cluster, for suspicious SQL activity using the vendor's example check `grep -i "COPY. TO PROGRAM" mail_logs`; any hit warrants investigation. Because a successful attacker holds root and can wipe or alter on-box evidence, also examine network and firewall logs held off the device for unexpected outbound uploads to external IP addresses or downloads from unknown hosts. Cisco has published Snort coverage (rules 67109 and 67110) that can help flag exploitation attempts.

Assume Compromise Where Indicators Appear: If exploitation is suspected on a physical appliance, preserve forensic evidence and engage Cisco TAC for support. For a virtual appliance, capture forensic information first, then rebuild from a fixed image, restore the configuration cleanly, and renew all credentials and cryptographic material stored on the device, since anything held on a compromised gateway should be considered exposed.

Reduce the Appliance's Exposure: Keep the management interface off the public internet, restrict administrative access to known trusted hosts, separate mail and management traffic onto different network interfaces, place the appliance behind a filtering firewall, and disable any services that are not required, such as HTTP and FTP. These hardening steps shrink the attack surface and limit how far an intruder can move if a gateway is targeted.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Defense Evasion	T1070: Indicator Removal	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX

References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX

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

September 16, 2026 • 07:30 AM

More at www.hivepro.com