



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Wednesday September 16, 2026

CAL-CSIC-202609-A-008

Critical SQL Injection Vulnerability on Cisco AsyncOS and Secure Email Gateway

Remote Code Execution

Zero-Day Vulnerability

Actively Exploited

Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) have identified a critical vulnerability, CVE-2026-76461, affecting Cisco AsyncOS Software for Cisco Secure Email Gateway (formerly IronPort ESA). CVE-2026-76461 is an SQL injection vulnerability (CWE-89) in the email parsing logic that allows an unauthenticated remote attacker to execute arbitrary SQL statements and run commands with root privileges on the underlying operating system. Successful exploitation requires no authentication, administrative access, or user interaction; which can lead to arbitrary SQL execution and ultimately command execution with root privileges on the underlying operating system.¹ The vulnerability carries a CVSS v3.1 base score of 9.8 (Critical)² and has been added to the CISA Known Exploited Vulnerabilities (KEV)³ catalog due to active exploitation in the wild. No verified public Proof-of-Concept (PoC) has been released.

The Cal-CSIC recommends the following:⁴

1. Verify Updates: Ensure all virtual and physical Cisco Secure Email Gateways to the fixed Cisco AsyncOS release specified in the vendor advisory.
2. Restart Browser: Have User Fully close and restart Chrome to load the latest patch.
3. Verify system integrity and monitor outbound network connections from gateway management interfaces.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

Affected Components and Versions

Affected Product	Affected Software	Versions Impacted
Cisco Secure Email Gateway	Cisco AsyncOS	Earlier than 16.5.0-780 Earlier than 16.0.4-3021 Earlier than 15.5.5-0141

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

References:

¹ SOCRadar; "CVE-2026-76461 Cisco Email Gateway Flaw Exploited"; <https://socradar.io/blog/cve-2026-76461-cisco-email-gateway-flaw/>; accessed 16 September 2026

² NIST; "CVE-2026-76461 Detail"; <https://nvd.nist.gov/vuln/detail/cve-2026-76461>; accessed 16 September 2026

³ CISA; "Known Exploited Vulnerabilities Catalog"; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-76461; accessed 16 September 2026

⁴ Cisco; "Cisco Secure Email Gateway SQL Injection Vulnerability"; <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX>; accessed 16 September 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR