



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



# CYBER ADVISORY

Wednesday, December 17, 2025

CAL-CSIC-202512-A-011

## Remote Execution Vulnerability Affecting Multiple Cisco Products

Remote Code Execution

Cisco AsyncOS

Established Persistence

Zero-Day in the Wild

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability that affects Cisco Secure Email Gateway (SEG) and Cisco Secure Email and Web Manager (SEWM) appliances. CVE-2025-20393 carries a CVSS 3.1 score of 10.0.<sup>1</sup> If successfully exploited, the vulnerability allows an attacker to execute arbitrary commands with *root* privileges and establish persistence on the underlying operating system of an affected appliance.<sup>2</sup> CVE-2025-20393 is known to be exploited in the wild, likely as a zero-day vulnerability, as there is currently no patch available or a workaround that directly mitigates the risk. Cisco states that they are tracking a campaign that is targeting Cisco AsyncOS Software for Cisco SEW and Cisco SEWM.

Cisco has stated that this vulnerability only affects Cisco SEG and Cisco SEWM appliances with non-standard configurations, when the Spam Quarantine feature is enabled and public-facing.<sup>3</sup>

The Cal-CSIC recommends immediately following Cisco's guidance to identify compromised appliances and multi-step processes to rebuild and restore impacted appliances.

**Analyst Comment:** Talos has stated that they have been aware of this exploitative activity since December 10, 2025, which has been ongoing since at least late November 2025. Continued exploitation of this vulnerability is likely due to the recent discovery of this new campaign and the lack of direct remediation/mitigation.

For further information on CVE-2025-20393 and Cisco's security advisory, please use this link:

[Cisco Secure Email Gateway And Cisco Secure Email and Web Manager](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4)

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4>

**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 Products:**

This vulnerability affects *all* releases of Cisco AsyncOS Software running Cisco SEG and Cisco SEWM

---

## **References**

---

<sup>1</sup> CVE.org; CVE-2025-20393; <https://www.cve.org/CVERecord?id=CVE-2025-20393>; accessed 17 December 2025

<sup>2</sup> Cisco; Reports About Cyberattacks Against Cisco Secure Email Gateway And Cisco Secure Email and Web Manager; <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4>; accessed 17 December 2025

<sup>3</sup> CiscoTalos; Threat Advisory; <https://blog.talosintelligence.com/uat-9686/>; accessed 17 December 17, 2025

**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**