Security Advisory 2025-042

Critical Vulnerability in Cisco Secure Email and Web Manager

2025-12-18 — v1.0

TLP:CLEAR

History:

- *18/12/2025 — v1.0 – Initial publication*

Summary

On December 17, 2025, Cisco released a security advisory for a critical vulnerability affecting Cisco Secure Email Gateway and Cisco Secure Email and Web Manager products [1].

It is recommended to follow Cisco's recommendations to check whether vulnerable appliances have been compromised, and to remediate the issue. There is no patch available for this vulnerability yet.

Technical Details

While there is not much technical details about the vulnerability **CVE-2025-20393**, with a CVSS score of 10, Cisco reveals that it allows attackers to execute arbitrary commands with root privileges on the underlying operating system of an affected appliance.

Affected Products

This vulnerability affects Cisco Secure Email Gateway, both physical and virtual, and Cisco Secure Email and Web Manager appliances, both physical and virtual, when both of the following conditions are met [1]:

- The appliance is configured with the Spam Quarantine feature.
- The Spam Quarantine feature is exposed to and reachable from the internet.

Recommendations

It is recommended to check if Cisco Secure Email Gateway and Cisco Secure Email and Web Manager appliances are configured with the Spam Quarantine feature, and if they are, that the feature is not reachable from the internet. If it is the case, it is recommended to open a Cisco Technical Assistance Center (TAC) case to verify whether an appliance has been compromised [1].

It is also recommended to follow Cisco's recommendations to remediate the issue [1]:

- Restore the appliance to a secure configuration when possible.
- Restrict access to the appliance and implement robust access control mechanisms.

In case the appliance was found to be compromised, it is recommended to investigate further any lateral movement that may have occurred within the network.

References

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4#vp