Active Exploitation of Cisco Secure Email Gateway Zero-Day Allows Root-Level Compromise

TL;DR

Cisco confirmed active exploitation of CVE-2025-20393 (CVSS 10), a zero-day affecting Cisco Secure Email Gateway and Cisco Secure Email and Web Manager.

Attackers are gaining unauthenticated, root-level command execution on exposed appliances and planting persistent backdoors.

There is no patch available yet. If Spam Quarantine is exposed to the internet, assume risk and apply mitigations immediately.

Overview

Cisco published an advisory due to an active attack campaign targeting Cisco Secure Email Gateway (SEG) and Cisco Secure Email and Web Manager (SEWM) appliances running AsyncOS. The activity was first identified on December 10 during a TAC support case and has been traced back to at least late November. The vulnerability, tracked as CVE-2025-20393 (CVSS 10), is caused by improper input validation in AsyncOS and allows an unauthenticated attacker to execute arbitrary operating system commands with root-level privileges.

Affected Products

- Cisco Secure Email Gateway (physical and virtual)
- Cisco Secure Email and Web Manager (physical and virtual)

Conditions required for exploitation

- Spam Quarantine feature is enabled
- Spam Quarantine is exposed to and reachable from the internet

Not affected

- Cisco Secure Email Cloud
- Cisco Secure Web

CVE-2025-20393 is only reachable when the Spam Quarantine feature is enabled and exposed to the internet. While this feature is not turned on by default and is not intended to be internet-facing, Cisco confirmed that all AsyncOS versions are affected when these configuration conditions are met. Exploitation does not require valid credentials or user interaction, allowing attackers to compromise exposed appliances quickly and quietly.

Cisco's investigation confirmed that the attackers are not stopping at initial access. Compromised appliances were modified to maintain long-term control through custom persistence mechanisms, covert access channels, and log manipulation designed to

reduce visibility. Cisco Talos attributes the activity with moderate confidence to a Chinese-nexus threat actor tracked as UAT-9686, noting overlap in tooling and behavior with activity previously linked to APT41 and UNC5174.

Observed Threat Activity

- AquaShell – custom backdoor used to maintain persistent access
- AquaTunnel – reverse SSH tunneling implant
- Chisel – tunneling utility used for traffic proxying
- AquaPurge – tool used to selectively remove log entries

Currently, there is no patch available and Cisco has stated that rebuilding affected appliances is the only confirmed way to fully remove attacker persistence following a compromise. If this vulnerability is exploited, an attacker gains root-level control of the email security appliance and can keep that access hidden over time. That foothold gives them visibility into mail flow and a quiet path deeper into the environment. Aspire recommends applying mitigations immediately.

Aspire Protects

- **Patch** – Cisco has not released a patch for CVE-2025-20393 at this time. Until fixed software becomes available, risk reduction depends on configuration changes and access controls.
    - Cisco advises the following:
    - Remove internet exposure from Spam Quarantine and management interface
    - Restrict access to trusted hosts using firewalls and access controls
    - Avoid direct internet-facing deployments of SEG and SEWM
    - Separate mail-handling and management interfaces
    - Review and retain logs for abnormal access or traffic
    - Disable unnecessary services such as HTTP and FTP
    - Rotate administrator credentials and tighten account permissions
    - Use strong authentication methods such as SAML or LDAP
    - **Monitor Cisco advisories for an upcoming patch**.

***Please Note**: This isn't a firewall bug. Firewalls are part of the mitigation because they can prevent internet access to the vulnerable interface.*

TTPs

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker exploited CVE-2025-20393 through internet-exposed Spam Quarantine interfaces to gain unauthenticated access to Cisco Secure Email Gateway and Secure Email and Web Manager appliances.

Execution

- Command and Scripting Interpreter: Unix Shell [T1059.004] – After exploitation, the attacker executed operating system commands as root within the AsyncOS environment.

Persistence

- Server Software Component [T1505] – The attacker installed a custom persistence mechanism (AquaShell) to maintain long-term access to the compromised appliance.

Defense Evasion

- Indicator Removal on Host [T1070.004] – Log manipulation tools were used to remove or alter log entries, limiting visibility into attacker activity.

IoCs

File Hashes

- AquaTunnel (ReverseSSH-based tunneling tool)
  - 2db8ad6e0f43e93cc557fbda0271a436f9f2a478b1607073d4ee3d20a87ae7ef
- AquaPurge (log manipulation utility)
  - 145424de9f7d5dd73b599328ada03aa6d6cdcee8d5fe0f7cb832297183dbe4ca
- Chisel (TCP/UDP tunneling tool)
  - 85a0b22bd17f7f87566bd335349ef89e24a5a19f899825b4d178ce6240f58bfc

IP Addresses

- 172[.]233[.]67[.]176
- 172[.]237[.]29[.]147
- 38[.]54[.]56[.]95

Behavioral and Logging IoCs

- Unexpected HTTP POST requests targeting the Spam Quarantine or other AsyncOS UI paths, especially those triggering root actions or shell execution.
- Outbound SSH or unusual tunneling activity potentially tied to reverse tunnels like AquaTunnel or Chisel.
- Gaps or suspicious deletions in logs, consistent with log-purging actions by tools like AquaPurge.

The complete list of IoCs for CVE-2025-20393 can be found in this GitHub repository.

Targeted Industries

This activity threatens organizations running Cisco Secure Email Gateway or Cisco Secure Email and Web Manager appliances, particularly those with internet-exposed Spam Quarantine configurations.

- Government
- Education
- Energy
- Healthcare
- Retail
- Finance
- Technology
- Legal
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

- Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.

- Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Reports About Cyberattacks Against Cisco Secure Email Gateway And Cisco Secure Email and Web Manager

UAT-9686 actively targets Cisco Secure Email Gateway and Secure Email and Web Manager

IOCs/2025/12 at main · Cisco-Talos/IOCs · GitHub