

CVE-2025-20393: Cisco AsyncOS Zero-Day Impacts Secure Email Appliances

 socradar.io/blog/cve-2025-20393-cisco-asyncos-zero-day-email

Ameer Owda

December 18, 2025



Recently, Cisco confirmed active exploitation of a previously unknown, **maximum-severity vulnerability** affecting Cisco Secure Email Gateway and Cisco Secure Email and Web Manager appliances running AsyncOS. The flaw, tracked as CVE-2025-20393, is already being abused in real-world attacks and allows threat actors to gain deep control over affected systems.

Enterprise [email security](#) solutions are widely relied on to stop phishing, malware, and data loss, which makes this disclosure especially relevant for security teams. Moreover, CISA guidance now requires U.S. government agencies to take action, making this issue an immediate operational priority.

This blog answers key questions about what the vulnerability is, how it is being exploited, who is at risk, and what organizations can do now to reduce exposure.

What is CVE-2025-20393?

CVE-2025-20393 (CVSS 10.0) is a zero-day vulnerability in Cisco AsyncOS Software, the operating system used by Cisco Secure Email Gateway and Cisco Secure Email and Web Manager. The flaw stems from improper input validation, which enables attackers to execute

arbitrary commands with root-level privileges on the underlying operating system.

This level of access effectively removes most security boundaries on the appliance. An attacker can modify system files, install additional tooling, and establish long-term persistence.

**CVE-2025-20393**
Critical Severity

 SVRS 96/100

 CVSSv3 10.0/10

 EPSS /1

TAGS

CISA KEV

In The Wild

VECTOR STRING

CVSS:3.1

AV:N

AC:L

PR:N

UI:N

S:C

C:H

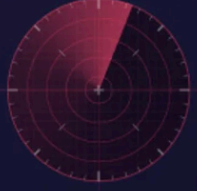
I:H

A:H

PUBLICATION DATE 2025-12-17LAST MODIFIED 2025-12-17

Details of CVE-2025-20393 (SOCRadRadar Vulnerability Intelligence)

As of this disclosure, Cisco has not released a patch for the vulnerability.

**Every second,
a dark web threat
makes a move**

Act before them

Start Dark Web Monitoring Trial

Which Cisco Products Are Affected?

Not all Cisco email security deployments are equally exposed. In its [advisory](#), Cisco has described the attacks as targeting a **limited subset of appliances** with exposed ports.

The affected products include Cisco Secure Email Gateway and **Cisco Secure Email and Web Manager**, in both physical and virtual forms. Cisco has also confirmed that all releases of Cisco AsyncOS Software are affected by this vulnerability.

Which Configurations Are Vulnerable to CVE-2025-20393?

According to Cisco, exploitation requires a specific configuration scenario. Successful exploitation depends on two conditions being met:

1. The **Spam Quarantine feature** must be enabled.
2. The Spam Quarantine interface **must be exposed** to and reachable from the internet.

The Spam Quarantine feature is not enabled by default, and Cisco deployment guides do not recommend exposing it directly to the internet. Cisco's investigation indicates that appliances with non-standard or overly permissive configurations are the ones observed to be compromised. Cisco Secure Email Cloud is not affected, and Cisco Secure Web products are not known to be impacted.

Who is Behind the Attacks Targeting Cisco AsyncOS Zero-Day?

[Cisco Talos](#) attributes the activity, with moderate confidence, to a China-nexus advanced persistent threat actor tracked as **UAT-9686**. The campaign has been **active since at least late November 2025** and was uncovered during a Cisco support case investigation on December 10, 2025.

The tooling and operational patterns observed in this activity overlap with those of other known Chinese threat groups. Some of the tools used in these attacks have previously been associated with actors such as [APT41](#) and UNC5174. The focus on email security and management solutions aligns with a broader trend of targeting perimeter systems that provide deep visibility into enterprise environments.

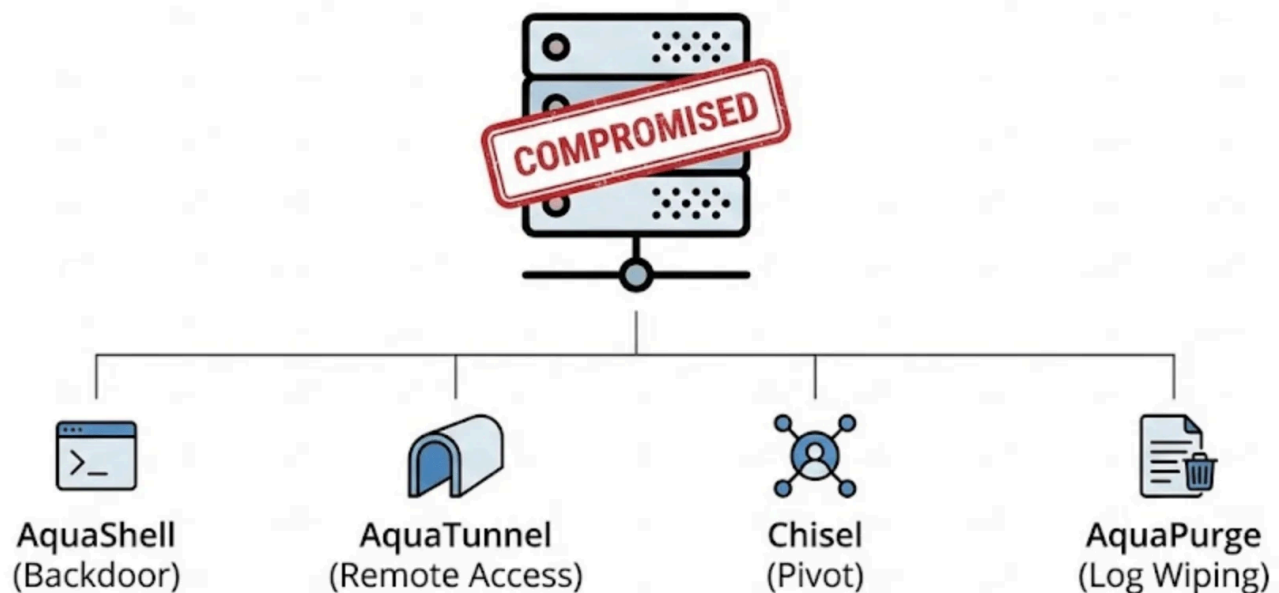
How Are Attackers Maintaining Persistence on Compromised Appliances?

Once access is obtained, the attackers move quickly to maintain long-term control. Cisco confirmed that compromised appliances contained custom persistence mechanisms designed to survive reboots and routine administrative actions.

One of the main tools observed is **AquaShell**, a lightweight Python-based backdoor embedded into an existing web application file. AquaShell listens for specially crafted, unauthenticated HTTP POST requests and decodes incoming data before executing commands in the system shell.

Additional tooling supports stealth and remote access:

- **AquaTunnel** establishes reverse SSH connections to attacker-controlled infrastructure.
- **Chisel** enables HTTP-based tunneling that can be used to pivot into internal networks.
- **AquaPurge** is used to selectively remove log entries, complicating forensic analysis and detection efforts.



Tools used in campaign targeting AsyncOS zero-day (CVE-2025-20393)

CISA Lists Cisco AsyncOS Zero-Day in Known Exploited Vulnerabilities

Following confirmation of active exploitation, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2025-20393 to its [Known Exploited Vulnerabilities \(KEV\)](#) catalog. This designation signals that the flaw is being used in real-world attacks and requires prioritized remediation.

CISCO | MULTIPLE PRODUCTS



Cisco Multiple Products Improper Input Validation Vulnerability: *Cisco Secure Email Gateway, Secure Email, AsyncOS Software, and Web Manager appliances contains an improper input validation vulnerability that allows threat actors to execute arbitrary commands with root privileges on the underlying operating system of an affected appliance.*

Related CWE: [CWE-20](#)

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

■ **Date Added:** 2025-12-17

■ **Due Date:** 2025-12-24

[Additional Notes +](#)

CISA KEV listing for CVE-2025-20393

Under Binding Operational Directive requirements, Federal Civilian Executive Branch (FCEB) agencies must apply mitigations for CVE-2025-20393 by **December 24, 2025**. While the mandate applies specifically to U.S. federal agencies, [KEV](#) inclusion is widely used by other organizations as a benchmark for vulnerability prioritization.

How Can Organizations Determine If They Are Exposed?

Organizations can begin by verifying whether the Spam Quarantine feature is enabled and exposed. This requires logging into the web management interface and reviewing the network interface configuration associated with Spam Quarantine.

Beyond configuration checks, administrators should review web and system logs for unexpected HTTP POST requests, unusual outbound connections, or signs of log manipulation. Because attackers attempted to clean logs, missing or incomplete records may also indicate malicious activity. Cisco recommends exporting logs to an external system to support deeper investigation.

At present, rebuilding the appliance is the only reliable method to fully remove attacker persistence once it has been confirmed.

Indicators of compromise (IOCs) associated with this campaign are provided at the end of this blog post to support detection and investigation efforts.

What Immediate Steps Should Defenders Take?

At the time of disclosure, no workaround fully mitigates the vulnerability itself. However, Cisco has outlined several defensive actions that can significantly reduce risk.

Administrators should remove direct internet exposure from management and Spam Quarantine interfaces wherever possible. Appliances should be placed behind [firewalls](#) that restrict access to trusted hosts only, and mail-handling functions should be separated from management interfaces.

Additional recommendations include:

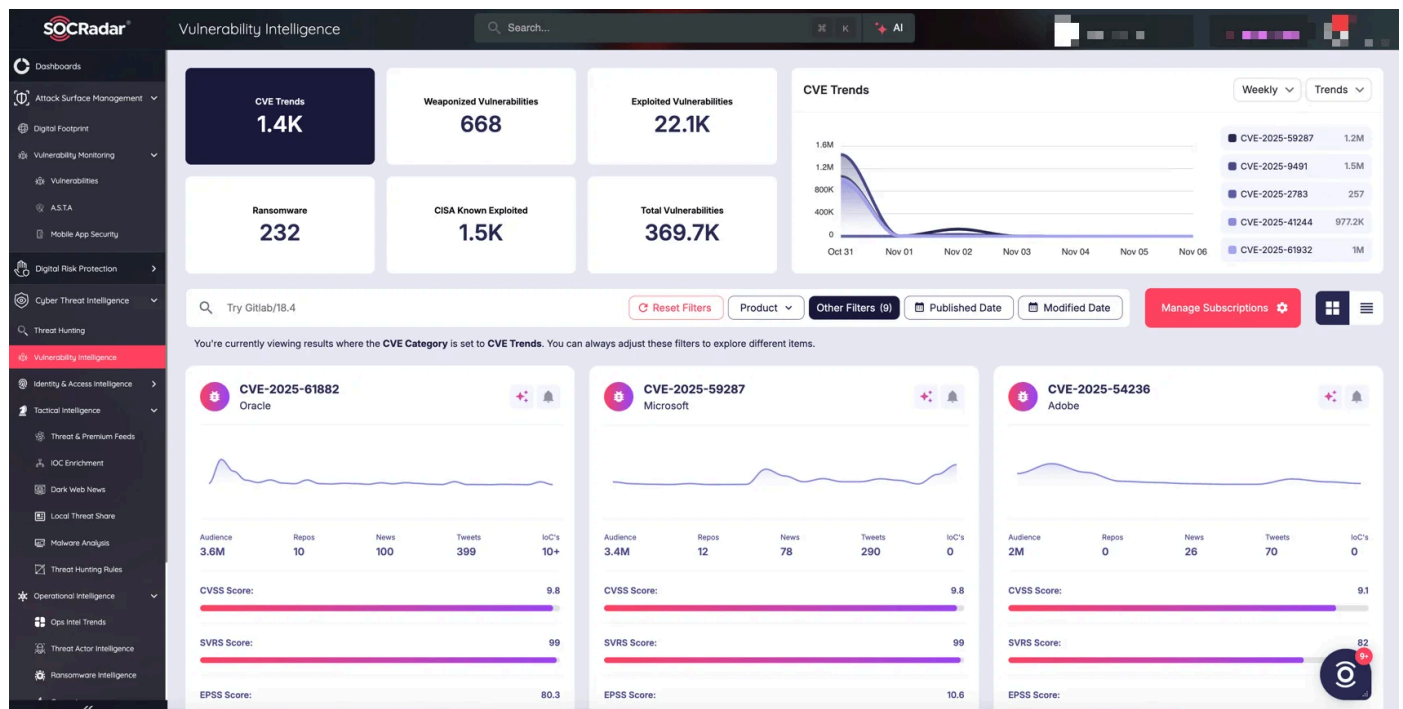
- disabling unnecessary services such as HTTP and FTP,
- enforcing strong authentication methods like SAML or LDAP,
- and replacing default administrator [credentials](#) with stronger alternatives.

These measures reduce the attack surface and make exploitation more difficult while organizations wait for permanent remediation.

How Can SOCRadar Help?

Active exploitation of zero-day vulnerabilities like CVE-2025-20393 highlights the challenge of tracking threats that emerge before patches or signatures are available. Security teams often need early visibility into exploitation trends, exposed assets, and related indicators to respond effectively.

SOCRadar's [Cyber Threat Intelligence](#) and [Attack Surface Management](#) modules help organizations monitor actively exploited vulnerabilities, track KEV-listed CVEs, and identify exposed or misconfigured assets that could be targeted in similar campaigns. By correlating vulnerability data with threat actor activity and external exposure, SOCRadar enables teams to prioritize remediation efforts and reduce risk during the critical window of exploitation.



SOCRadar's Vulnerability Intelligence

Indicators of Compromise (IOCs)

The following indicators of compromise were observed by [Cisco Talos](#) during its investigation into the CVE-2025-20393 exploitation campaign.

File Hashes:

AquaTunnel (ReverseSSH-based tool)

2db8ad6e0f43e93cc557fbda0271a436f9f2a478b1607073d4ee3d20a87ae7ef

AquaPurge (log-cleaning utility)

145424de9f7d5dd73b599328ada03aa6d6cdcee8d5fe0f7cb832297183dbe4ca

Chisel (tunneling tool)

85a0b22bd17f7f87566bd335349ef89e24a5a19f899825b4d178ce6240f58bfc

IP Addresses:

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

Organizations detecting these indicators should assume a high risk of compromise and initiate incident response procedures, including isolating affected systems and engaging Cisco TAC for further guidance.



The banner features a red target icon on the left. To its right, the text "Cyber Threat Intelligence" is displayed in a large, bold font, with "Cyber Threat" in dark blue and "Intelligence" in red. Further right, a smaller line of text reads "Your Shield Against Cyber Adversaries is even stronger now!" with a red underline. At the bottom right, there is a red button with the text "→ Get Free Access".

Cyber Threat Intelligence

Your Shield Against Cyber Adversaries is even stronger now!

→ Get Free Access