

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **CVE-2025-20393: Critical Cisco AsyncOS Zero-Day Actively Exploited**

Date of Publication

December 19, 2025

Last Updated Date

January 21, 2026

Admiralty Code

A1

TA Number

TA2025384

# Summary

**First Seen:** Late November 2025

**Affected Products:** Cisco Secure Email Gateway (SEG) & Cisco Secure Email and Web Manager (SEWM)

**Affected Platforms:** Cisco AsyncOS Software (physical and virtual appliances)

**Threat Actor:** UAT-9686

**Malware:** AquaShell, AquaTunnel, AquaPurge, and Chisel

**Impact:** CVE-2025-20393 is a critical zero-day vulnerability (CVSS 10.0) in Cisco AsyncOS affecting Cisco Secure Email Gateway and Secure Email and Web Manager appliances. The flaw in the Spam Quarantine web interface allows unauthenticated remote attackers to execute arbitrary commands with root privileges when the interface is internet-exposed. It has been actively exploited since late November 2025 by the China-linked APT group UAT-9686 using advanced persistence malware. Cisco released security patches on January 15, 2026, and organizations are strongly urged to upgrade to the fixed software releases immediately.

## 🔧 CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-20393	Cisco Multiple Products Improper Input Validation Vulnerability	Cisco Multiple Products	✔️	✔️	✔️

## 🗡️ Exploitation Timeline



# Vulnerability Details

## #1

CVE-2025-20393 is a critical zero-day vulnerability (CVSS 10.0) affecting Cisco Secure Email Gateway (SEG) and Cisco Secure Email and Web Manager (SEWM) appliances running Cisco AsyncOS. The flaw arises from improper input validation (CWE-20) in the Spam Quarantine web interface, allowing unauthenticated remote attackers to execute arbitrary commands with root privileges. Exploitation is possible only when the Spam Quarantine feature is enabled and its interface is exposed to the internet, an unsafe but commonly misconfigured deployment scenario.

## #2

The vulnerability has been actively exploited since late November 2025 by UAT-9686, a China-linked advanced persistent threat group with tooling overlaps to APT41 and UNC5174. Cisco Talos identified the campaign on December 10, 2025, during an investigation of a TAC support case. Attackers leverage the flaw for initial access and then deploy a tailored malware toolkit designed for stealth and long-term appliance control.

## #3

Post-exploitation activity includes the deployment of AquaShell (a Python-based web backdoor), AquaTunnel (a Go-based reverse SSH tunneling tool), AquaPurge (a log-clearing utility), and Chisel (an HTTP tunneling tool). These components provide persistence, command-and-control, lateral movement capabilities, and anti-forensic functionality. Cisco has stated that these persistence mechanisms cannot be reliably removed and that full appliance rebuilds are required to eradicate confirmed compromises.

## #4

On January 15, 2026, Cisco released security patches and updated the advisory to Version 2.0 (Final). Organizations are strongly urged to upgrade to the fixed software releases immediately. The patch addresses the exploited vulnerability and removes the persistence mechanisms installed by threat actors. In addition to patching, organizations should continue enforcing network-level mitigations, including restricting internet exposure to the Spam Quarantine interface, enforcing strict firewall controls, separating mail and management interfaces, and exporting logs to external systems to support detection and forensic analysis.

# Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-20393	Cisco Secure Email Gateway (SEG): Versions prior to 15.0.5-016, 15.5.4-012, 16.0.4-016 Cisco Secure Email and Web Manager (SEWM): Versions prior to 15.0.2-007, 15.5.4-007, 16.0.4-010	cpe:2.3:a:cisco:secure_email_and_web_manager_virtual_appliance:-:*:*:*:*:*:* cpe:2.3:a:cisco:secure_email_gateway_virtual_appliance:-:*:*:*:*:*:* cpe:2.3:h:cisco:secure_email_and_web_manager:-:*:*:*:*:*:* cpe:2.3:h:cisco:secure_email_gateway:-:*:*:*:*:*:* cpe:2.3:o:cisco:asynocos:*:*:*:*:*:*	CWE-20

## Recommendations



**Apply Security Patches Immediately:** Upgrade to the fixed AsyncOS releases. The patch addresses the vulnerability and removes persistence mechanisms deployed by threat actors.



**Restrict Spam Quarantine Interface Access:** Immediately remove or block internet access to the Spam Quarantine web interface. Configure firewall rules to allow connections only from trusted internal IP addresses. This is the most critical mitigation as the vulnerability requires the interface to be internet-exposed for remote exploitation.



**Implement Network Segmentation:** Deploy Cisco Secure Email Gateway and SEWM appliances behind dedicated filtering firewalls. Separate mail processing and management functions onto different network interfaces. This limits attacker lateral movement and reduces the attack surface if compromise occurs.



**Hunt for Indicators of Compromise:** Monitor network traffic for connections to known C2 infrastructure. Check file integrity of `/data/web/euq_webui/htdocs/index.py` for unauthorized modifications. Investigate any unusual outbound SSH connections from email appliances.



**Enable External Log Forwarding:** Configure log export to external SIEM or syslog servers immediately. UAT-9686 deploys AquaPurge to clear local logs and destroy forensic evidence. External log storage ensures attack artifacts are preserved for incident response and investigation.



**Rebuild Confirmed Compromised Appliances:** If exploitation is detected, perform a complete appliance rebuild from clean images. Standard remediation procedures will not remove UAT-9686 persistence mechanisms including AquaShell and AquaTunnel.

## Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0011</u></b> Command and Control
<b><u>TA0003</u></b> Persistence	<b><u>TA0005</u></b> Defense Evasion	<b><u>T1203</u></b> Exploitation for Client Execution	<b><u>T1140</u></b> Deobfuscate/Decode Files or Information
<b><u>T1068</u></b> Exploitation for Privilege Escalation	<b><u>T1588.005</u></b> Exploits	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1588</u></b> Obtain Capabilities
<b><u>T1090</u></b> Proxy	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1059.006</u></b> Python
<b><u>T1505.003</u></b> Web Shell	<b><u>T1505</u></b> Server Software Component	<b><u>T1070.002</u></b> Clear Linux or Mac System Logs	<b><u>T1070</u></b> Indicator Removal
<b><u>T1572</u></b> Protocol Tunneling	<b><u>T1095</u></b> Non-Application Layer Protocol	<b><u>T1027</u></b> Obfuscated Files or Information	

## Indicators of Compromise (IOCs)

TYPE	VALUE
<b>SHA256</b>	2db8ad6e0f43e93cc557fbda0271a436f9f2a478b1607073d4ee3d20a87ae7ef, 145424de9f7d5dd73b599328ada03aa6d6cdcee8d5fe0f7cb832297183dbe4ca, 85a0b22bd17f7f87566bd335349ef89e24a5a19f899825b4d178ce6240f58bfc
<b>IPv4</b>	172[.]233[.]67[.]176, 172[.]237[.]29[.]147, 38[.]54[.]56[.]95
<b>File Path</b>	/data/web/euq_webui/htdocs/index.py

## Patch Details

Upgrade to fixed releases:

Cisco Secure Email Gateway: 15.0.5-016, 15.5.4-012, or 16.0.4-016;

Cisco Secure Email and Web Manager: 15.0.2-007, 15.5.4-007, or 16.0.4-010.

Link:

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

## References

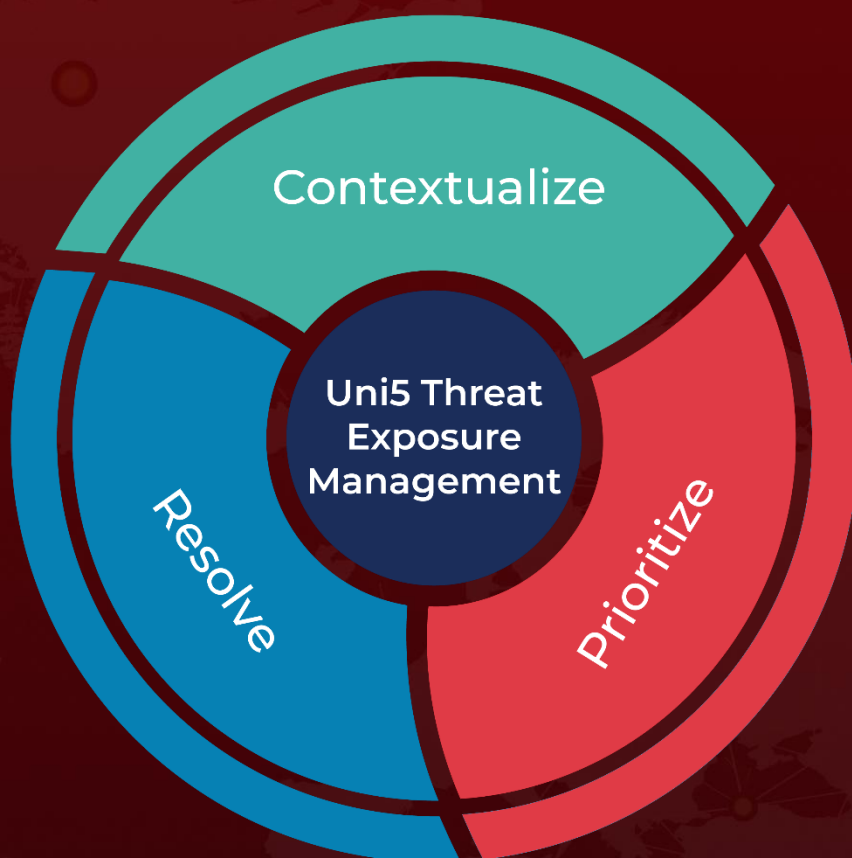
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4>

<https://blog.talosintelligence.com/uat-9686/>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**December 19, 2025 • 5:00 AM**

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)