Zero-Day Crisis: CVE-2025-20393 Unpatched on Cisco Email Gateways, Exploited by China-Linked Hackers

By Santosh Sethuraman

Published: 2025-12-23 · Archived: 2026-04-05 18:09:37 UTC

Network edge devices continue to be a primary target for sophisticated state-sponsored actors aiming to bypass traditional perimeter defenses. Recent disclosures reveal a critical zero-day vulnerability in Cisco's Secure Email Gateway (SEG) and Secure Web Manager (SMA) appliances is being actively exploited by a suspected Chinese threat group to establish deep persistence within high-value networks.

At the center of this activity is a highly sophisticated espionage campaign attributed to the threat cluster tracked as **UAT-9686** . Exploiting a critical flaw in the Cisco AsyncOS Spam Quarantine interface, these actors are deploying a custom malware suit, including the **AquaShell** malware, to maintain long-term root access and pivot into internal networks.

Background on UAT-9686 Operations

UAT-9686 is a suspected Chinese state-sponsored threat group with a history of targeting networking infrastructure and edge appliances. Unlike financially motivated cybercriminals, UAT-9686 operations are characterized by:

- **Zero-Day Discovery:** Capability to identify and weaponize unknown vulnerabilities in proprietary network appliances.

- **Custom Tooling:** Development of specialized malware (AquaShell, AquaPurge) tailored for specific operating systems like Cisco AsyncOS.
- **Stealth & Anti-Forensics:** Heavy emphasis on log manipulation and "living off the land" to evade detection.
- **Deep Persistence:** establishing footholds that survive reboots and standard security scans.

In this specific campaign, the group has focused on bypassing authentication mechanisms in the Spam Quarantine feature to gain root-level control over email security appliances, effectively turning security tools into espionage platforms.

Campaign Overview

The UAT-9686 campaign demonstrates a methodical effort to compromise the communication infrastructure of targeted organizations.

Primary Targets

- Telecommunications and critical infrastructure sectors.
- Organizations utilizing Cisco Secure Email Gateway (ESA) and Secure Email and Web Manager (SMA).

Key Characteristics

- Exploitation of the **Spam Quarantine interface** (Port 6025) via HTTP packet manipulation.
- Deployment of Python-based malwares directly onto the appliance.
- Use of specialized "wiper" tools to selectively scrub forensic evidence.

Vulnerabilities Details

The campaign relies on a critical zero-day vulnerability that allows remote code execution (RCE) with root privileges.

- **Vulnerability ID:** CVE-2025-20393
- **Affected Products**: Cisco AsyncOS versions up to and including 16.0.3-044 on Cisco Secure Email Gateway and Cisco Secure Email and Web Manager
- **CVSS Score:** 10.0 (Critical)
- **EPSS Score:** 4.56%

Infection Method

Initial Access

Attackers target the **Spam Quarantine** feature enabled on the management interface of the Cisco appliance. By sending specially crafted, unauthenticated HTTP POST requests to the exposed service (typically on port 6025), the attackers trigger an improper input validation flaw.

Exploitation

Successful exploitation grants the attacker **root-level privileges** on the underlying AsyncOS operating system.

This allows them to bypass the restricted CLI typically available to administrators and interact directly with the OS shell.

Payload Delivery
Once root access is achieved, UAT-9686 deploys a suite of custom Python scripts. Since AsyncOS includes a Python interpreter by default, these scripts execute natively without requiring external dependencies, reducing the forensic footprint.

Execution & Persistence
The actors utilize a modular malware toolkit to maintain control:

- **AquaShell:** A custom Python malware that acts as a passive listener. It allows attackers to execute arbitrary system commands covertly.
- **AquaTunnel:** A tool designed to establish reverse SSH tunnels, ensuring persistent remote access even if the appliance is behind a firewall.
- **Chisel:** The open-source tunneling tool is often deployed alongside custom malware to facilitate traffic routing and lateral movement into the internal network.

Defense Evasion
To avoid detection, the group deploys **AquaPurge**, a specialized log-wiping utility. AquaPurge selectively removes entries related to the attacker's activities from system logs while leaving legitimate traffic intact, complicating incident response efforts.

Command-and-Control (C2)
Command-and-control is achieved through passive listening malwares (AquaShell) that avoid beaconing, and encrypted tunnels (AquaTunnel/Chisel) to route traffic through SSH channels.

MITRE ATT&CK Techniques

Tactic	Technique	Description
Initial Access	**T1190:** Exploit Public-Facing App	Exploiting exposed Spam Quarantine (Port 6025).
Privilege Escalation	**T1068:** Exploitation for Privilege Escalation	Exploiting CVE-2025-20393 for root access.
Execution	**T1059.006:** Python Scripting	Native Python execution for AquaShell.
Persistence	**T1572:** Protocol Tunneling	Reverse SSH tunnels via AquaTunnel.
Defense Evasion	**T1070:** Indicator Removal on Host	AquaPurge wipes logs and forensics.

Command & Control	**T1105:** Ingress Tool Transfer	Dropping custom scripts onto appliance.
Lateral Movement	**T1573:** Encrypted Channel	Chisel tunnels traffic internally.

Visual Flow

Internet (Attacker) -> **Port 6025** (Spam Quarantine Exploit) -> **Root Access** (AsyncOS) -> **Drop AquaShell/AquaPurge** -> **Log Wiping** (Anti-Forensics) -> **Reverse SSH Tunnel** -> **Internal Network Access**

Mitigation Steps

Given that this vulnerability was exploited as a zero-day, immediate mitigation is critical.

- **Disable Spam Quarantine:** If not strictly necessary, disable the Spam Quarantine feature on the ESA/SMA appliances immediately.
- **Restrict Access (ACLs):** If the feature is required, use firewall rules or Access Control Lists (ACLs) to block access to port **6025** from the public internet. Ensure only trusted internal management IPs can access this port.
- **Monitor System Logs:** While AquaPurge attempts to scrub logs, look for gaps in logging, unexpected Python process execution, or unauthorized SSH connections initiated from the appliance.
- **Isolate Management Interfaces:** Ensure the management interface is physically or logically separated from the public network and strictly VPN-gated.

Instantly Fix Risks with Saner Patch Management

Saner patch management is a continuous, automated, and integrated software that instantly fixes risks exploited in the wild. The software supports major operating systems like Windows, Linux, and macOS, as well as 550+ third-party applications.

It also allows you to set up a safe testing area to test patches before deploying them in a primary production environment. Saner patch management additionally supports a patch rollback feature in case of patch failure or a system malfunction.

Experience the fastest and most accurate patching software here.

Read more articles
