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

By Cisco Talos

Published: 2025-12-17 · Archived: 2026-04-05 15:36:43 UTC

Wednesday, December 17, 2025 11:55

- Cisco Talos recently discovered a campaign targeting Cisco AsyncOS Software for Cisco Secure Email Gateway, formerly known as Cisco Email Security Appliance (ESA), and Cisco Secure Email and Web Manager, formerly known as Cisco Content Security Management Appliance (SMA).
- We assess with moderate confidence that the adversary, who we are tracking as UAT-9686, is a Chinese-nexus advanced persistent threat (APT) actor whose tool use and infrastructure are consistent with other Chinese threat groups.
- As part of this activity, UAT-9686 deploys a custom persistence mechanism we track as “AquaShell” accompanied by additional tooling meant for reverse tunneling and purging logs.
- Our analysis indicates that appliances with non-standard configurations, as described in Cisco's advisory, are what we have observed as being compromised by the attack.

Cisco Talos is tracking the active targeting of Cisco AsyncOS Software for Cisco Secure Email Gateway, formerly known as Cisco Email Security Appliance (ESA), and Cisco Secure Email and Web Manager, formerly known as Cisco Content Security Management Appliance (SMA), enabling attackers to execute system-level commands and deploy a persistent Python-based backdoor, AquaShell. Cisco became aware of this activity on December 10, which has been ongoing since at least late November 2025. Additional tools observed include AquaTunnel (reverse SSH tunnel), chisel (another tunneling tool), and AquaPurge (log-clearing utility). Talos' analysis indicates that appliances with non-standard configurations, as described in Cisco's advisory, are what we have observed as being compromised by the attack.

The Cisco Secure Email and Web Manager centralizes management and reporting functions across multiple Cisco Email Security Appliances (ESAs) and Web Security Appliances (WSAs), offering centralized services such as spam quarantine, policy management, reporting, tracking, and configuration management to simplify administration and enhance security enforcement.

Customers are strongly advised to follow the guidance published in the security advisories discussed below. Additional recommendations specific to Cisco are available here.

Talos assesses with moderate confidence that this activity is being conducted by a Chinese-nexus threat actor, which we track as UAT-9686. We have observed overlaps in tactics, techniques and procedures (TTPs), infrastructure, and victimology between UAT-9686 and other Chinese-nexus threat actors Talos tracks. Tooling used by UAT-9686, such as AquaTunnel (aka ReverseSSH), also aligns with previously disclosed Chinese-nexus

APT groups such as APT41 and UNC5174. Additionally, the tactic of using a custom-made web-based implant such as AquaShell is increasingly being adopted by highly sophisticated Chinese-nexus APTs.

AquaShell

AquaShell is a lightweight Python backdoor that is embedded into an existing file within a Python-based web server. The backdoor is capable of receiving encoded commands and executing them in the system shell. It listens passively for unauthenticated HTTP POST requests containing specially crafted data. If such a request is identified, the backdoor will then attempt to parse the contents using a custom decoding routine and execute them in the system shell.

AquaShell is delivered as an encoded data blob that is decoded and ultimately placed in "/data/web/euq_webui/htdocs/index.py".

The result of decoding the data blob is the Python code that constitutes the AquaShell backdoor. AquaShell parses the HTTP POST request, decodes it using a combination custom algorithm and Base64 decoding and executes the resulting commands on the appliance.

AquaPurge

AquaPurge removes lines containing specific keywords from the log files specified. It uses the "egrep" command to filter out (invert search) all content that doesn't contain the keywords and then simply commits them to the log files:

```
#!/bin/sh
commandlog='/data/log/heimdall/commandd/commandd.current'
cpt="<keyword>"
euqguilog='/data/pub/euqgui_logs/euqgui.current'
ept="{REDACTED}"

CMD

(sleep 10 && ls ${commandlog} 2>/dev/null&& egrep ${cpt} ${commandlog} >/dev/null &&
echo "$(cat ${commandlog} | egrep -v ${cpt})" > ${commandlog} &)
(sleep 10 && ls ${euqguilog} 2>/dev/null&& egrep ${ept} ${euqguilog} >/dev/null &&
echo "$(cat ${euqguilog} | egrep -v ${ept})" > ${euqguilog} &)

rm -f /data/tmp/PKGFILE
rm -rf /data/tmp/BINDIR
exit 0
```

AquaTunnel

AquaTunnel is a compiled GoLang ELF binary based on the open-source "ReverseSSH" backdoor. AquaTunnel creates a reverse SSH connection from the compromised system back to an attacker-controlled server, enabling unauthorized remote access even when the system is behind firewalls or NAT.

Chisel

Chisel is an open-source tunneling tool that supports creating TCP/UDP tunnels over a single-port HTTP-based connection. Chisel allows an attacker to proxy traffic through a compromised edge device, allowing them to easily pivot through that device into the internal environment.

Recommendations for Cisco customers are available here. If your organization does find connections to the provided actor indicators of compromise (IOCs), please open a case with Cisco TAC.

All IOCs, including IPs and file hashes determined to be associated with this campaign have been blocked across the Cisco portfolio.

IOCs

The IOCs can also be found in our GitHub repository here.

AquaTunnel

2db8ad6e0f43e93cc557fbda0271a436f9f2a478b1607073d4ee3d20a87ae7ef

AquaPurge

145424de9f7d5dd73b599328ada03aa6d6cdcee8d5fe0f7cb832297183dbe4ca

Chisel

85a0b22bd17f7f87566bd335349ef89e24a5a19f899825b4d178ce6240f58bfc

172[.]233[.]67[.]176

172[.]237[.]29[.]147

38[.]54[.]56[.]95
