Boletín de alerta

Boletín Nro.: 104
Fecha de publicación: 18/12/2025
Tema: Alerta 2025-104 Vulnerabilidad ZeroDay Crítica en Productos Cisco explotado en campañas de ataque.
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Esta campaña de ataque afecta a Cisco Secure Email Gateway, tanto físico como virtual, y a los dispositivos Cisco Secure Email y Web Manager, tanto físicos como virtuales, cuando se cumplen las dos condiciones siguientes:

- El dispositivo está configurado con la función **de cuarentena de spam**.
- La función **de cuarentena de spam** está expuesta y se puede acceder a ella desde Internet.

Nota: Todas las versiones del software Cisco AsyncOS se ven afectadas por esta campaña de ataque.

Aun Cisco investiga la vulnerabilidad y el ataque.

Descripción

Se ha reportado la explotación activa de un Zero Day en productos Cisco que aún no cuenta con un parche disponible. Esta campaña de ciberataques está dirigida a un subconjunto limitado de dispositivos con ciertos puertos expuestos a Internet que ejecutan el software Cisco AsyncOS para Cisco Secure Email Gateway y Cisco Secure Email and Web Manager. Esta vulnerabilidad se ha identificado como CVE-2025-20393 y cuenta con una puntuación CVSSv3 de 10. Aún se encuentra bajo investigación, por lo que se esperan nuevas actualizaciones con el paso de las horas.

Esta vulnerabilidad permite a los cibercriminales ejecutar comandos arbitrarios con privilegios de root en el sistema operativo subyacente de un dispositivo afectado. La investigación en curso ha revelado evidencia de un mecanismo de persistencia implementado por los atacantes para mantener cierto control sobre los dispositivos comprometidos.

La vulnerabilidad afecta a Cisco Secure Email Gateway, tanto físico como virtual, y a los dispositivos Cisco Secure Email and Web Manager, también físicos y virtuales, cuando se cumplen simultáneamente las siguientes dos condiciones, las cuales no están configuradas por defecto:

- El dispositivo está configurado con la función de cuarentena de spam.

- La función de cuarentena de spam está expuesta y es accesible desde Internet.

El equipo de seguridad Cisco Talos está rastreando el ataque activo contra el software Cisco AsyncOS para Cisco Secure Email Gateway (anteriormente conocido como Cisco Email Security Appliance, ESA) y Cisco Secure Email and Web Manager (anteriormente conocido como Cisco Content Security Management Appliance, SMA). La explotación de esta vulnerabilidad permite a los atacantes ejecutar comandos a nivel de sistema e implementar una puerta trasera persistente basada en Python, denominada AquaShell.

Cisco detectó esta actividad el 10 de diciembre, la cual ha estado activa al menos desde finales de noviembre de 2025. Otras herramientas observadas incluyen AquaTunnel (túnel SSH inverso), Chisel (otra herramienta de tunelización) y AquaPurge (utilidad de borrado de registros). El análisis de Talos indica que los dispositivos con configuraciones no estándar, como se describe en este aviso, son los que se han observado como vulnerables al ataque.

Útiles:

- **Determinar si la cuarentena de spam está habilitada en un dispositivo Cisco Secure Email Gateway**

Para determinar si la función de Cuarentena de Spam está configurada y habilitada en un dispositivo, conéctese a la interfaz de administración web y navegue al siguiente menú: **Red** > **Interfaces IP >** [**Seleccione la interfaz en la que está configurada la Cuarentena de Spam**] **.** Si la casilla junto a Cuarentena de Spam está marcada, la función está habilitada.

- **Determinar si la cuarentena de spam está habilitada en un dispositivo Cisco Secure Email and Web Manager**

Para determinar si la función Cuarentena de spam está configurada y habilitada en un dispositivo, conéctese a la interfaz de administración web y navegue al siguiente menú: **Dispositivo de administración > Red** > **Interfaces IP >** [**Seleccione la interfaz en la que está configurada la Cuarentena de spam**]. Si la casilla de verificación junto a Cuarentena de spam está marcada, la función está habilitada.

IOC:

Los IOC también se pueden encontrar en el repositorio de GitHub de Talos .

- **Túnel acuático**

2db8ad6e0f43e93cc557fbda0271a436f9f2a478b1607073d4ee3d20a87ae7ef

- **Purga de agua**

145424de9f7d5dd73b599328ada03aa6d6cdcee8d5fe0f7cb832297183dbe4ca

- **Cincel**

85a0b22bd17f7f87566bd335349ef89e24a5a19f899825b4d178ce6240f58bfc

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

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

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

Recomendaciones:

Si se ha identificado que la interfaz de administración web o el puerto de cuarentena de spam de un dispositivo están expuestos y son accesibles desde internet, Cisco recomienda encarecidamente seguir un proceso de varios pasos para restaurar el dispositivo a una configuración segura, siempre que sea posible.

Para descargar dispositivos virtuales de reemplazo, visite la página de descarga de software de Cisco correspondiente:

- Puerta de enlace de correo electrónico seguro de Cisco
- Administrador web y de correo electrónico seguro de Cisco

Si no es posible restaurar el dispositivo, Cisco recomienda contactar con el TAC para verificar si ha sido comprometido. En caso de que se confirme la vulneración, reconstruir el dispositivo es, actualmente, la única opción viable para erradicar el mecanismo de persistencia de los actores de amenazas.

Además, Cisco recomienda encarecidamente restringir el acceso al dispositivo e implementar mecanismos de control de acceso sólidos para garantizar que los puertos no estén expuestos a redes no seguras.

Cisco aún no ha lanzado parches de seguridad, pero ha proporcionado una lista de recomendaciones generales para los productos afectados. Estas incluyen:

- **Restringir el acceso a Internet:** Evitar el acceso directo desde Internet o limitarlo a hosts conocidos y de confianza.
- **Proteger con firewall:** Utilizar un firewall para filtrar el tráfico hacia y desde los dispositivos, permitiendo solo conexiones de hosts conocidos y de confianza.
- **Separar funciones (solo para Cisco Secure Email Gateway):** Separar las funciones de correo y administración en interfaces de red distintas para reducir el acceso no autorizado.
- **Monitorear el tráfico:** Revisar periódicamente el tráfico del registro web en busca de actividad inesperada y enviar los registros a un servidor externo para su conservación.
- **Deshabilitar HTTP y servicios innecesarios:** Desactivar HTTP para el portal del administrador principal y otros servicios de red no esenciales como FTP.
- **Mantener el software actualizado:** Actualizar el dispositivo a la última versión del software Cisco AsyncOS.
- **Usar autenticación segura:** Implementar métodos de autenticación de usuario final seguros como SAML o LDAP.
- **Cambiar contraseñas y restringir acceso:** Modificar la contraseña de administrador predeterminada por una más segura y crear cuentas de usuario con acceso restringido.

- **Utilizar SSL/TLS:** Obtener un certificado SSL de una autoridad de certificación o crear uno autofirmado.

Para ver todas las recomendaciones puede redirigirse al siguiente enlace:

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

Información adicional:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4
- **https://nvd.nist.gov/vuln/detail/CVE-2025-20393**
- **https://blog.talosintelligence.com/uat-9686/**
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/ejecucion-remota-de-comandos-en-productos-de-cisco?sstc=u88504nl594112