Incidente ID:	0020
Fecha del reporte:	19/12/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad Software Cisco AsyncOS
Herramienta de detección	N/A
Activo involucrado:	Cisco
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la vulnerabilidad CVE-2025-20393 de nivel Critica (CVSS 10.0) la cual se está presentando en la interfaz de gestión basada en web de varios productos de Cisco. Se trata de un fallo de Inyección de Comandos (Command Injection) debido a una validación insuficiente de la entrada del usuario en ciertos endpoints de la API.

Descripción:

Cisco ha reportado una vulnerabilidad crítica de día cero rastreada como CVE-2025-20393 que está siendo explotada activamente por un grupo APT vinculado a China, UAT-9686, dirigido a Cisco Secure Email Gateway y Cisco Secure Email and Web Manager.

Se trata de una vulnerabilidad crítica (CVSS 10.0) en el software Cisco AsyncOS, que usan dispositivos como Cisco Secure Email Gateway y Cisco Secure Email and Web Manager para proteger y gestionar el correo electrónico corporativo. Esta falla de validación incorrecta de entradas permite que un atacante remoto, sin autenticación ni credenciales, ejecute comandos arbitrarios con acceso total (root) sobre el sistema afectado si el dispositivo tiene activada y accesible desde internet la función de Spam Quarantine.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Los investigadores también han encontrado evidencia de un mecanismo de persistencia colocado para mantener control sobre los dispositivos comprometidos. Instalando herramientas avanzadas de persistencia y acceso remoto. Entre ellas se encuentran AquaShell, un backdoor basado en Python que recibe comandos a través de HTTP; AquaTunnel, utilizado para crear túneles reversos y mantener acceso incluso detrás de firewalls; AquaPurge, diseñada para eliminar o manipular registros y dificultar la investigación forense; y Chisel, una herramienta de tunelización que permite profundizar el acceso dentro de la red comprometida.

La vulnerabilidad sigue sin parchearse y se debe a una validación de entrada incorrecta, permitiendo a los atacantes ejecutar comandos maliciosos con privilegios elevados en el sistema operativo subyacente.

Productos afectados:

La vulnerabilidad afecta a las siguientes líneas de productos si tienen habilitada la interfaz de administración web:

- Cisco Secure Email Gateway (todas las versiones de Cisco AsyncOS Software)
- Cisco Secure Email and Web Manager (todas las versiones de Cisco AsyncOS Software)

Modo de explotación y cadena de infección

Los adversarios utilizan las siguientes tácticas y técnicas para aprovechar este fallo:

- T1190 Exploit Public-Facing Application: Uso de la interfaz web expuesta para ganar acceso inicial.
- T1059.004 Command and Scripting Interpreter (Unix Shell): Ejecución de comandos directamente en la shell del dispositivo.
- T1068 Exploitation for Privilege Escalation: Obtención de privilegios de nivel "root" tras la inyección.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

El fallo reside en un componente encargado de procesar solicitudes HTTP específicas.

- El sistema no sanitiza adecuadamente los caracteres especiales o secuencias de comandos enviadas a través de parámetros de entrada.

- Un atacante envía una solicitud HTTP POST o GET especialmente diseñada hacia la IP de administración del dispositivo. Al incluir metacaracteres de shell (como ;, |, o &&), el atacante puede "romper" la instrucción legítima y forzar al sistema a ejecutar código malicioso.

Indicadores de Compromiso (IoCs)

Como parte de la campaña de ataque descrita en este aviso, el actor de amenazas plantó un canal encubierto persistente que se utilizó para acceder de forma remota al dispositivo comprometido.

Los clientes que deseen verificar explícitamente si un dispositivo ha sido comprometido pueden abrir un caso en el Centro de Asistencia Técnica (TAC) de Cisco. Para agilizar nuestra investigación sobre la posible vulneración, asegúrese de que el acceso remoto esté habilitado en los dispositivos afectados.

Adicionalmente, aunque al momento de la publicación de este boletín no se tiene todos los detalles técnicos completos de indicadores de compromiso (IOCs), se han publicado listas de hashes de archivos asociados con las herramientas maliciosas y direcciones IP vinculadas a la campaña UAT-9686, que pueden usarse en sistemas de detección para ayudar a identificar intrusiones:

AquaTunnel

- 2db8ad6e0f43e93cc557fbda0271a436f9f2a478b1607073d4ee3d20a87ae7ef

AquaPurge

- 145424de9f7d5dd73b599328ada03aa6d6cdcee8d5fe0f7cb832297183dbe4ca

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Chisel

- 85a0b22bd17f7f87566bd335349ef89e24a5a19f899825b4d178ce6240f58bfc
- 172.233.67.176
- 172.237.29.147
- 38.54.56.95

Recomendaciones de mitigación:

Cisco recomienda que 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.

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.

Otras recomendaciones generales son las siguientes:

- Impedir el acceso desde Internet al dispositivo. Si se requiere acceso a Internet desde éste, restringir el acceso solo a hosts conocidos y de confianza en los puertos/protocolos que se incluyen en las guías de usuario.

- Proteja los dispositivos Cisco Secure Email Gateway y Cisco Secure Email and Web Manager detrás de un dispositivo de filtrado, como un firewall, y filtre el tráfico hacia y desde los dispositivos, permitiendo solo que los hosts conocidos y de confianza envíen tráfico a los dispositivos.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- En el caso de Cisco Secure Email Gateway, separe las funciones de correo y gestión en interfaces de red independientes. Esto reduce la posibilidad de que usuarios no autorizados accedan a la red de gestión interna.

- Supervise periódicamente el tráfico del registro web para detectar cualquier tráfico inesperado hacia o desde los dispositivos. Los registros deben enviarse a un servidor externo, si es posible, y conservarse durante un tiempo suficiente para que se puedan realizar investigaciones posteriores al evento con datos de registro suficientes. Desactive HTTP para el portal del administrador.

Fuentes:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4
- https://www.ccn-cert.cni.es/es/seguridad-al-dia/alertas-ccn-cert/13121-ccn-cert-al-11-25-campana-activa-contra-cisco-secure-email-gateway-y-cisco-secure-email-and-web-manager.html
- https://socprime.com/es/blog/cve-2025-20393-vulnerability-exploitation/
- https://ciberseguridad.euskadi.eus/noticia/2025/campana-de-ciberataques-critica-contra-cisco-secure-email-gateway-y-web-manager/webcyb00-contcibglos/es/

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570