Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CÓMO EL MALWARE DRIPDROPPER SE PROPAGA EN LA NUBE A TRAVÉS DE UNA VULNERABILIDAD EN APACHE ACTIVEMQ

19/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

Recientemente investigadores han detectado una campaña activa donde cibercriminales están explotando una vulnerabilidad de hace casi 2 años en Apache ActiveMQ, Ah esta falla se le dio el ID de CVE-2023-46604 y tiene una puntuación de CVSS 10.0.

CÓMO EL MALWARE DRIPDROPPER SE PROPAGA EN LA NUBE A TRAVÉS DE UNA VULNERABILIDAD EN APACHE ACTIVEMQ

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_08_19_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	19/08/2025
Es día cero (0 day):	No

RESUMEN

Recientemente investigadores han detectado una campaña activa donde cibercriminales están explotando una vulnerabilidad de hace casi 2 años en Apache ActiveMQ, Ah esta falla se le dio el ID de CVE-2023-46604 y tiene una puntuación de CVSS 10.0.

Algo importante de recalcar es que una vez obtuvieron acceso los cibercriminales parcharon ellos mismos la vulnerabilidad para evitar que otros también la usaran y así dificultar el rastreo.
La vulnerabilidad es de tipo RCE que permite ejecución de código remoto en sistemas Linux en la nube.

¿Cómo funciona el ataque?

Los cibercriminales se aprovechan del broker de ActiveMQ para ejecutar comandos arbitrarios en el sistema, lo que les abre la puerta para tomar el control total del servidor.

Manipulación de servicios críticos: Una de las primeras acciones detectadas es la modificación del servicio SSH, habilitando el acceso como root. Esto les asegura una vía de entrada estable y de máximo privilegio.

Uso de malware modular (DripDropper):

- Este downloader malicioso necesita una contraseña para funcionar, lo que complica su análisis por parte de los investigadores.
- Se conecta a su infraestructura de mando y control (C2) utilizando servicios aparentemente legítimos, como Dropbox, desde donde descarga nuevas cargas maliciosas.

Malware desplegado: A través de DripDropper, los cibercriminales distribuyen diferentes amenazas, entre ellas:

- HelloKitty ransomware (cifrado de archivos y extorsión).
- Rootkits para Linux (ocultan la actividad maliciosa en el sistema).
- GoTitan, una botnet en expansión.
- Godzilla, una web shell usada para mantener el acceso remoto.

Persistencia en el sistema: Para asegurarse de que el malware siga activo incluso después de reinicios, los cibercriminales crean entradas en cron (/etc/cron.hourly, /etc/cron.daily, etc.), que ejecutan sus scripts maliciosos de manera periódica.

Autoparcheo para camuflarse: De forma irónica, los cibercriminales descargan parches oficiales desde repositorios como Apache Maven para cerrar la vulnerabilidad que usaron en primer lugar. Esto les permite ocultar el vector inicial de acceso, complicando la investigación forense.

¿Por qué es un caso relevante?

- Parchear tras la explotación demuestra sofisticación para evitar que otros actores también comprometan la misma infraestructura.
- Mezcla tráfico malicioso con comunicaciones comunes, dificultando la detección.
- El malware es modular, adaptable a diferentes endpoints.

Versiones afectas

- Apache ActiveMQ 5.x: desde la 5.0.0 hasta la 5.18.1 todas vulnerables.
- Apache ActiveMQ Legacy OpenWire Module: desde la 5.0.0 hasta la 5.18.1.
- Apache ActiveMQ Artemis NO está afectado.

El fallo fue corregido en ActiveMQ 5.15.16, 5.16.7, 5.17.6 y 5.18.2.

RECOMENDACIONES

- Instalar la última versión de Apache ActiveMQ publicada por el proyecto (parche oficial para CVE-2023-46604).
- Si no es posible actualizar de inmediato, aplicar los workarounds temporales que sugiere Apache, aunque no sustituyen la actualización.
- Revisar los logs de ActiveMQ y de SSH en busca de conexiones no autorizadas.
- Detectar cambios inesperados en configuraciones críticas, como el acceso root vía SSH.

NOTICIA COMPLETA

https://devel.group/blog/como-el-malware-dripdropper-se-propaga-en-la-nube-a-traves-de-una-vulnerabilidad-en-apache-activemq/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group