CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenazas cibernéticas

Fecha: 21/11/2023

Problemática: Kinsing explotó falla de seguridad crítica en servidores Apache ActiveMQ

Correlativo: AC-0096

Institución / Sector: Público y Privado

CONTEXTO

Grupo de amenazas Kinsing explotó activamente una falla de seguridad crítica en servidores Apache ActiveMQ vulnerables para infectar sistemas Linux con rootkits y mineros de criptomonedas. «CVE-2023-46604» permite la ejecución remota de código, permitiendo acceder al adversario para descargar e instalar el malware Kinsing.

SITUACIÓN

La vulnerabilidad, CVE-2023-46604, es una vulnerabilidad de ejecución remota de código (RCE) que permite a los atacantes ejecutar código arbitrario en un servidor Apache ActiveMQ vulnerable. Una vez que un servidor ActiveMQ ha sido comprometido, los atacantes pueden descargar e instalar el malware Kinsing en el sistema. Kinsing es un malware de Linux diseñado para la minería de criptomonedas. Una vez instalado, Kinsing comenzará a extraer criptomonedas en el sistema comprometido.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alta	Alta	Alta

IMPACTO

La explotación de esta vulnerabilidad podría tener un impacto significativo en las organizaciones que ejecutan servidores Apache ActiveMQ. Los atacantes podrían usar esta vulnerabilidad para comprometer sistemas Linux y extraer criptomonedas, provocando daños significativos en la infraestructura y en el rendimiento del sistema.

RECOMENDACIONES

- Actualizar a una versión parcheada de Apache ActiveMQ
- Realizar respaldos de la información de los sistemas de su organización en forma regular.
- Implementar medidas de seguridad adicionales para proteger sus servidores ActiveMQ, como la autenticación y el cifrado.
- Mantener el sistema de respaldos de forma separada.
- Mantener los sistemas actualizados a la última versión.

REFERENCIAS

The hacker News
https://thehackernews.com/2023/11/kinsing-hackers-exploit-apache-activemq.html