



El grupo de ransomware HelloKitty está explotando la vulnerabilidad de Apache ActiveMQ

Los expertos en ciberseguridad están emitiendo una advertencia sobre la presunta explotación de una recientemente divulgada vulnerabilidad crítica en el servicio de intermediación de mensajes de código abierto Apache ActiveMQ, la cual podría resultar en la ejecución de código remoto.

En un [informe](#) publicado el miércoles, la firma de ciberseguridad Rapid7 informa que *«en ambos casos, el adversario intentó implantar archivos binarios de ransomware en los sistemas objetivos con el fin de extorsionar a las organizaciones víctimas»*.

Basándose en la nota de rescate y la evidencia disponible, se atribuye esta actividad a la familia de ransomware HelloKitty, cuyo código fuente se filtró en un foro a principios de octubre.

Se informa que las intrusiones involucran la explotación de la [CVE-2023-46604](#), una vulnerabilidad de ejecución de código remoto en Apache ActiveMQ que permite a un actor de amenazas ejecutar comandos de shell arbitrarios.

Es importante destacar que esta [vulnerabilidad](#) tiene una puntuación CVSS de 10.0, lo que indica la máxima gravedad. Esta vulnerabilidad se ha corregido en las versiones de ActiveMQ 5.15.16, 5.16.7, 5.17.6 o 5.18.3 lanzadas a finales del mes pasado.

Las versiones afectadas por esta vulnerabilidad incluyen:

- Apache ActiveMQ 5.18.0 antes de la 5.18.3
- Apache ActiveMQ 5.17.0 antes de la 5.17.6
- Apache ActiveMQ 5.16.0 antes de la 5.16.7
- Apache ActiveMQ antes de la 5.15.16
- Apache ActiveMQ Legacy OpenWire Module 5.18.0 antes de la 5.18.3
- Apache ActiveMQ Legacy OpenWire Module 5.17.0 antes de la 5.17.6
- Apache ActiveMQ Legacy OpenWire Module 5.16.0 antes de la 5.16.7



El grupo de ransomware HelloKitty está explotando la vulnerabilidad de Apache ActiveMQ

- Apache ActiveMQ Legacy OpenWire Module 5.8.0 antes de la 5.15.16

Desde que se dio a conocer la vulnerabilidad, se ha hecho público un [código de explotación](#) de prueba de concepto (PoC) y [detalles técnicos adicionales](#). Rapid7 señala que el comportamiento observado en las dos redes víctimas es «*similar a lo que esperaríamos de la explotación de la CVE-2023-46604*».

La explotación exitosa lleva al adversario a intentar cargar archivos binarios remotos denominados M2.png y M4.png utilizando el Instalador de Windows (msiexec).

Ambos archivos MSI contienen un ejecutable .NET de 32 bits llamado dllloader, que a su vez carga una carga útil codificada en Base64 llamada EncDLL, que funciona de manera similar al ransomware. Esta carga útil busca y termina un conjunto específico de procesos antes de iniciar el proceso de cifrado y agrega la extensión «.locked» a los archivos cifrados.

La Fundación Shadowserver [informa](#) que encontró 3,326 [instancias de ActiveMQ accesibles](#) a través de Internet que son susceptibles a la CVE-2023-46604 a partir del 1 de noviembre de 2023. La mayoría de los servidores vulnerables se encuentran en China, Estados Unidos, Alemania, Corea del Sur e India.

Dada la explotación activa de esta vulnerabilidad, se recomienda encarecidamente a los usuarios que actualicen a la versión corregida de ActiveMQ lo más pronto posible y que realicen un escaneo en busca de indicadores de compromiso en sus redes.