Los expertos en ciberseguridad están alertando sobre un aumento notable en la actividad de actores maliciosos que están aprovechando activamente una vulnerabilidad ya parcheada en Apache ActiveMQ para desplegar la web shell Godzilla en sistemas comprometidos.

> *«Las shells web están ocultas en un formato binario desconocido y han sido diseñadas para evadir los escáneres de seguridad y aquellos basados en firmas. A pesar de que el formato binario es desconocido, el motor JSP de ActiveMQ sigue compilando y ejecutando la web shell»*, mencionó Trustwave.

CVE-2023-46604 (puntuación CVSS: 10.0) hace referencia a una grave vulnerabilidad en Apache ActiveMQ que permite la ejecución remota de código. Desde su divulgación pública a finales de octubre de 2023, ha sido activamente explotada por múltiples adversarios para instalar ransomware, rootkits, mineros de criptomonedas y botnets de DDoS.

En el conjunto más reciente de intrusiones observado por Trustwave, las instancias vulnerables han sido atacadas con shells web basadas en JSP que se insertan en el directorio de instalación de ActiveMQ bajo la carpeta «admin».

La web shell, conocida como Godzilla, es una puerta trasera con amplias funcionalidades capaz de analizar solicitudes HTTP POST entrantes, ejecutar el contenido y devolver los resultados en forma de una respuesta HTTP.

> *«Lo que hace que estos archivos maliciosos sean particularmente notables es la forma en que el código JSP parece estar oculto en un tipo de binario desconocido. Este método tiene el potencial de eludir medidas de seguridad, escapando a la detección por parte de puntos finales de seguridad durante el escaneo»,* señaló el investigador de seguridad Rodel Mendrez.

Una inspección más detallada de la cadena de ataque revela que el código de la web shell se

transforma en código Java antes de su ejecución mediante el Motor Servlet Jetty.

En última instancia, la carga útil JSP permite al actor de amenazas conectarse a la web shell a través de la interfaz de usuario de gestión de Godzilla y obtener control total sobre el sistema objetivo, facilitando la ejecución de comandos de shell arbitrarios, la visualización de información de red y la realización de operaciones de gestión de archivos.

Se recomienda encarecidamente a los usuarios de Apache ActiveMQ que actualicen a la última versión lo antes posible para mitigar posibles amenazas.