Los investigadores en ciberseguridad han revelado que los atacantes pueden aprovechar instancias mal configuradas de la Consola de Scripts de Jenkins para llevar a cabo actividades delictivas como la minería de criptomonedas.

> *«Las malas configuraciones, como los mecanismos de autenticación configurados incorrectamente, exponen el punto final '/script' a los atacantes. Esto puede resultar en la ejecución remota de código (RCE) y en el uso indebido por parte de actores maliciosos»,* explicaron Shubham Singh y Sunil Bharti de Trend Micro en un informe técnico publicado la semana pasada.

Jenkins, una plataforma popular de integración continua y entrega continua (CI/CD), cuenta con una consola de scripts Groovy que permite a los usuarios ejecutar scripts Groovy arbitrarios dentro del entorno de ejecución del controlador de Jenkins.

Los encargados del proyecto, en la documentación oficial, destacan que la shell Groovy basada en la web puede usarse para leer archivos que contienen datos sensibles (por ejemplo, «/etc/passwd»), descifrar credenciales configuradas en Jenkins e incluso reconfigurar configuraciones de seguridad.

La consola *«no ofrece controles administrativos para evitar que un usuario (o administrador) pueda afectar todas las partes de la infraestructura de Jenkins una vez que puede ejecutar la Consola de Scripts,»* señala la documentación. *«Conceder acceso a la Consola de Scripts a un usuario normal de Jenkins es esencialmente lo mismo que otorgarle derechos de Administrador dentro de Jenkins.»*

Aunque el acceso a la Consola de Scripts generalmente está limitado a usuarios autenticados con permisos administrativos, las instancias de Jenkins mal configuradas podrían hacer que el punto final «/script» (o «/scriptText») sea accesible en internet, lo que lo hace susceptible de ser explotado por atacantes que buscan ejecutar comandos peligrosos.

Trend Micro reportó que detectó casos en los que actores maliciosos explotaban la mala

configuración del plugin Groovy de Jenkins para ejecutar una cadena codificada en Base64 que contiene un script malicioso diseñado para minar criptomonedas en el servidor comprometido, desplegando un minero alojado en berrystore[.]me y estableciendo persistencia.

> *«El script se asegura de que tiene suficientes recursos del sistema para realizar la minería de manera efectiva. Para lograr esto, el script verifica los procesos que consumen más del 90% de los recursos de la CPU y procede a finalizar estos procesos. Además, terminará todos los procesos detenidos»,* señalaron los investigadores.

Para protegerse contra estos intentos de explotación, se recomienda asegurar una configuración adecuada, implementar autenticación y autorización sólidas, realizar auditorías regulares y restringir la exposición pública de los servidores Jenkins en internet.

Este descubrimiento se produce en un contexto de aumento de robos de criptomonedas resultantes de hacks y explotaciones en la primera mitad de 2024, lo que ha permitido a los actores maliciosos robar $1.38 mil millones, frente a los $657 millones del año anterior.

> *«Los cinco principales hacks y explotaciones representaron el 70% del monto total robado hasta ahora este año. Las violaciones de claves privadas y frases de recuperación siguen siendo un vector de ataque principal en 2024, junto con explotaciones de contratos inteligentes y ataques de préstamos rápidos»,* señaló la plataforma de inteligencia blockchain TRM Labs.