Una vulnerabilidad de seguridad recientemente descubierta en OSGeo GeoServer GeoTools ha sido utilizada en varias campañas para desplegar mineros de criptomonedas, malware de botnets como Condi y JenX, así como un backdoor conocido como SideWalk.

El fallo de seguridad es una vulnerabilidad crítica de ejecución remota de código (CVE-2024-36401, con una puntuación CVSS de 9.8), que permitiría a atacantes tomar el control de instancias vulnerables.

A mediados de julio, la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA) lo incluyó en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), basándose en pruebas de que está siendo activamente explotada. La Fundación Shadowserver informó que detectó intentos de explotación contra sus sensores honeypot desde el 9 de julio de 2024.

Según Fortinet FortiGuard Labs, se ha visto que la vulnerabilidad se está utilizando para distribuir GOREVERSE, un servidor proxy inverso diseñado para establecer comunicación con un servidor de comando y control (C2) y realizar actividades después de la explotación inicial.

Se cree que estos ataques tienen como objetivo proveedores de servicios de TI en la India, empresas tecnológicas en Estados Unidos, entidades gubernamentales en Bélgica y compañías de telecomunicaciones en Tailandia y Brasil.

El servidor GeoServer también ha sido utilizado para la distribución de Condi, una variante de la botnet Mirai conocida como JenX, y al menos cuatro tipos de mineros de criptomonedas. Uno de estos mineros se descarga desde un sitio web falso que imita al Instituto de Contadores Públicos de la India (ICAI).

Una de las cadenas de ataques más destacadas que explota esta vulnerabilidad es la que propaga un avanzado backdoor para Linux llamado SideWalk, que se atribuye a un grupo de amenazas chino identificado como APT41.

El ataque comienza con un script en shell que descarga los binarios ELF para las arquitecturas ARM, MIPS y X86, los cuales extraen el servidor C2 de una configuración cifrada, se conectan a él y reciben instrucciones adicionales para ejecutar en el dispositivo comprometido.

Esto incluye el uso de una herramienta legítima llamada Fast Reverse Proxy (FRP) para evitar la detección mediante la creación de un túnel cifrado entre el host y el servidor controlado por el atacante, lo que permite un acceso remoto persistente, la exfiltración de datos y el despliegue de nuevas cargas maliciosas.

> *«Los principales objetivos parecen estar distribuidos en tres regiones clave: América del Sur, Europa y Asia»,* indicaron los investigadores de seguridad Cara Lin y Vincent Li.
>
> *«Esta distribución geográfica sugiere una campaña de ataques sofisticada y extendida, que posiblemente explota vulnerabilidades comunes en estos mercados diversos o se enfoca en industrias específicas de estas áreas».*

Este avance se produce mientras CISA ha añadido recientemente a su catálogo KEV dos vulnerabilidades descubiertas en 2021 en DrayTek VigorConnect (CVE-2021-20123 y CVE-2021-20124, con puntuaciones CVSS de 7.5), que podrían ser utilizadas para descargar archivos arbitrarios del sistema operativo subyacente con privilegios de root.