Los hackers están armando activamente servidores sin parches afectados por la vulnerabilidad Log4Shell, recientemente identificada en Log4j, para instalar mineros de criptomonedas, Cobalt Strike, y reclutar los dispositivos en una botnet, incluso cuando las señales de telemetría apuntan a la explotación de la vulnerabilidad nueve días antes de que ocurra.

Netlab, la división de seguridad de redes de Qihoo 360, reveló que las amenazas como Mirai y Muhstik (también conocido como Tsunami), están apuntando a sistemas vulnerables para propagar la infección y aumentar su poder de cómputo para orquestar la denegación de servicio distribuida (DDoS) con el objetivo de inutilizar al objetivo. Muhstik fue visto antes explotando una vulnerabilidad de seguridad crítica en Atlassian Confluence (CVE-2021-26084 con puntuación CVSS de 9.8) a inicios de septiembre.

Este último desarrollo se produce cuando se descubrió que la vulnerabilidad ha estado bajo ataque durante al menos más de una semana antes de su divulgación pública el 10 de diciembre, y compañías como Auvik, ConnectWise Manage y N-able confirmaron que sus servicios se han visto afectados, lo que amplía el alcance de la vulnerabilidad a más fabricantes.

> *«La evidencia más temprana que hemos encontrado hasta ahora del exploit Log4j es 2021-12-01 04:36:50 UTC. Esto sugiere que estuvo en estado salvaje al menos nueve días antes de la divulgación pública. Sin embargo, no se ve evidencia de explotación masiva hasta después de la divulgación pública»,* dijo Cisco Talos en un informe independiente.

Con el número de rastreo CVE-2021-44228 y puntuación CVSS de 10.0, la vulnerabilidad se refiere a un caso de ejecución remota de código en Log4j, un marco de registro Apache de código abierto basado en Java ampliamente utilizado en entornos empresariales para registrar eventos y mensajes generados por aplicaciones de software.

Todo lo que se requiere de un adversario para aprovechar la vulnerabilidad es enviar una

cadena especialmente diseñada que contiene el código malicioso que se registra en Log4j versión 2.0 o superior, lo que permite al actor de amenazas cargar código arbitrario de un dominio controlado por el atacante en un servidor susceptible y tomar el control.

> *«La mayor parte de los ataques que Microsoft ha observado en este momento han estado relacionados con el escaneo masivo por parte de atacantes que intentan utilizar huellas digitales en sistemas vulnerables, así como el escaneo por parte de compañías e investigadores de seguridad. Según la naturaleza de la vulnerabilidad, una vez que el atacante tiene acceso y control total de una aplicación, puede realizar una miríada de objetivos»*, dijo el Equipo de Inteligencia de Amenazas de Microsoft 365 Defender.

Particularmente, la compañía dijo que detectó una gran cantidad de actividades maliciosas, incluida la instalación de Cobalt Strike para permitir el robo de credenciales y el movimiento lateral, la implementación de mineros de criptomonedas y la extracción de datos de las máquinas comprometidas.

Esta situación también ha dejado a las empresas luchando por implementar soluciones para el error. El proveedor de seguridad de red SonicWall, en un aviso, reveló que su solución de seguridad de correo electrónico se ve afectada, asegurando que está trabajando para lanzar una solución para el problema mientras sigue investigando el resto de su línea. El proveedor de tecnología de virtualización VMware, también advirtió sobre *«intentos de explotación en la naturaleza»*, y agregó que está lanzando parches a varios de sus productos.

En todo caso, incidentes como estos muestran cómo una sola falla, cuando se descubre en paquetes incorporados en una gran cantidad de software, puede tener efectos dominó, actuando como un canal para futuros ataques y representando un riesgo crítico para los sistemas afectados.

> *«Todos los agentes de amenaza necesitan solo una línea de texto para*

> *desencadenar un ataque. No hay un objetivo obvio para esta vulnerabilidad: los hackers están adoptando un enfoque de rociar y orar para causar estragos»,* dijo el investigador senior de seguridad de Huntress Labs, John Hammond.