La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), junto con el Comando Cibernético de la Guardia Costera (CGCYBER), emitieron el jueves una advertencia conjunta sobre los continuos intentos por parte de los atacantes de amenazas de explotar la vulnerabilidad Log4Shell en los servidores VMware Horizon para violar redes objetivo.

> *«Desde diciembre de 2021, varios grupos de atacantes han explotado Log4Shell en servidores VMware Horizon de cara al público sin parches. Como parte de la explotación, los presuntos actores de APT implantaron malware de cargador en sistemas comprometidos con ejecutables integrados que permiten el comando y control remoto (C2)»,* dijeron las agencias.

En un caso, se dice que el adversario pudo moverse lateralmente dentro de la red de la víctima, obtener acceso a una red de recuperación de desastres y recopilar y filtrar datos confidenciales de las fuerzas del orden.

Log4Shell, rastreada como CVE-2021-44228 (puntuación CVSS: 10.0), es una vulnerabilidad de ejecución remota de código que afecta a la biblioteca de registro Apache Log4j que utiliza una amplia gama de consumidores y servicios empresariales, sitios web, aplicaciones y otros productos.

La explotación exitosa de la vulnerabilidad podría permitir que un atacante envíe un comando especialmente diseñado a un sistema afectado, lo que permite a los atacantes ejecutar código malicioso y tomar el control del objetivo.

Con base en la información recopilada como parte de los compromisos de respuesta a incidentes, las agencias dijeron que los atacantes armaron el exploit para lanzar cargas maliciosas, incluidos los scripts de PowerShell y una herramienta de acceso remoto denominada «hmsvc.exe» que está equipada con capacidades para registrar pulsaciones de teclas e implementar más programas maliciosos.

> *«El malware puede funcionar como un proxy de tunelización C2, lo que permite que un operador remoto pase a otros sistemas y avance más en una red. También ofrece un acceso a la interfaz gráfica de usuario (GUI) a través de un sistema Windows de destino»,* dijeron las agencias.

Los scripts de PowerShell, observados en el entorno de producción de una segunda organización, facilitaron el movimiento lateral, lo que permitió a los atacantes de APT implantar malware de carga que contenía ejecutables que incluyen la capacidad de monitorear de remotamente el escritorio de un sistema, obtener acceso de shell inverso, filtrar datos y cargar y ejecutar binarios de siguiente etapa.

Además, el grupo de hackers aprovechó CVE-2022-22954, una vulnerabilidad de ejecución remota de código en VMware Workspace ONE Access e Identity Manager, que salió a la luz en abril de 2022, para entregar el sehll web Dingo J-spy.

La actividad continua relacionada con Log4Shell incluso después de más de seis meses sugiere que la vulnerabilidad es de gran interés para los hackers, incluidos los actores de amenazas persistentes avanzadas (APT) patrocinados por el estado, que han apuntado de forma oportunista a servidores sin parches para obtener un punto de apoyo inicial para la actividad de seguimiento.

Según la compañía de seguridad cibernética ExtraHop, las vulnerabilidades de Log4j han estado sujetas a incesantes intentos de escaneo, con los sectores financiero y de salud emergiendo como un mercado descomunal para posibles ataques.

> *«Log4j está aquí para quedarse, veremos a los atacantes aprovechándolo una y otra vez. Log4j se enterró profundamente en capas y capas de código compartido de terceros, lo que nos lleva a la conclusión de que veremos instancias de la vulnerabilidad de Log4j explotadas en servicios utilizados por organizaciones que usan una gran cantidad de código abierto»,* dijo Randori, de IBM, en un informe de abril de 2022.