La Agencia de Seguridad Cibernética e Infraestructura de los Estados Unidos (CISA) emitió una advertencia el jueves, alertando sobre la explotación de vulnerabilidades de seguridad en Fortinet FortiOS SSL-VPN y Zoho ManageEngine ServiceDesk Plus por parte de múltiples actores estatales. Estos actores están aprovechando las vulnerabilidades para obtener acceso no autorizado y establecer una presencia persistente en sistemas comprometidos.

> De acuerdo con una alerta conjunta publicada por CISA, el FBI y la Fuerza de Misión Nacional de Ciberseguridad (CNMF), *«actores de amenazas persistentes avanzadas respaldados por naciones-estado aprovecharon CVE-2022-47966 para obtener acceso no autorizado a una aplicación de cara al público (Zoho ManageEngine ServiceDesk Plus), establecer una presencia persistente y moverse lateralmente dentro de la red».*

Aunque no se han revelado las identidades de los grupos de amenazas detrás de estos ataques, el Comando de Ciberseguridad de Estados Unidos (USCYBERCOM) sugiere la posible implicación de equipos estatales iraníes.

Estos hallazgos se basan en una investigación de incidentes llevada a cabo por CISA en una organización del sector aeronáutico no identificada, realizada de febrero a abril de 2023. Existe evidencia que sugiere que la actividad maliciosa podría haber comenzado ya el 18 de enero de 2023.

CVE-2022-47966 se refiere a una vulnerabilidad crítica de ejecución de código remoto que permite a un atacante no autenticado tomar el control total de las instancias vulnerables.

Una vez que se logra la explotación exitosa de CVE-2022-47966, los actores de amenazas obtienen acceso de nivel de root al servidor web y proceden a descargar malware adicional, enumerar la red, recopilar credenciales de usuario administrativas y moverse lateralmente dentro de la red.

No está claro de inmediato si se ha sustraído información propietaria como resultado de

estos ataques.

Se informa que la entidad en cuestión también fue comprometida mediante un segundo vector de acceso inicial que involucraba la explotación de CVE-2022-42475, una vulnerabilidad grave en Fortinet FortiOS SSL-VPN, para acceder al firewall.

> CISA declaró: *«Se identificó que los actores de APT comprometieron y utilizaron credenciales de cuenta administrativa legítimas pero deshabilitadas de un contratista previamente contratado, a pesar de que la organización había confirmado que el usuario había sido deshabilitado antes de la actividad observada».*

Los atacantes también han sido observados iniciando múltiples sesiones cifradas de Transport Layer Security (TLS) hacia varias direcciones IP, lo que sugiere transferencia de datos desde el dispositivo del firewall. Además, aprovechan credenciales válidas para saltar desde el firewall hacia un servidor web y desplegar shells web para obtener acceso de puerta trasera.

En ambos casos, se informa que los adversarios desactivaron las credenciales de cuenta administrativa y borraron registros de varios servidores críticos en el entorno, en un intento por eliminar el rastro forense de sus actividades.

> CISA señaló: *«Entre principios de febrero y mediados de marzo de 2023, se detectó el archivo anydesk.exe en tres hosts. Los actores de APT comprometieron uno de los hosts y se movieron lateralmente para instalar el ejecutable en los otros dos».*

Actualmente no se sabe cómo se instaló AnyDesk en cada máquina. Otra táctica utilizada en los ataques involucra el uso del cliente legítimo ConnectWise ScreenConnect para descargar y ejecutar la herramienta de volcado de credenciales Mimikatz.

Además, los actores intentaron explotar una conocida vulnerabilidad en Apache Log4j (CVE-2021-44228 o Log4Shell) en el sistema ServiceDesk como punto de acceso inicial, aunque sin éxito.

Dado el continuo aprovechamiento de estas vulnerabilidades de seguridad, se recomienda a las organizaciones que apliquen las últimas actualizaciones, monitoreen el uso no autorizado de software de acceso remoto y eliminen cuentas y grupos innecesarios para prevenir su abuso.