Hasta cinco familias distintas de software malicioso fueron utilizadas por presuntos actores respaldados por un estado, como parte de actividades de post-explotación que aprovecharon dos vulnerabilidades de día cero en los dispositivos de VPN Ivanti Connect Secure (ICS) desde principios de diciembre de 2023.

«Estas familias permiten a los actores de amenazas evadir la autenticación y abrir un acceso trasero a estos dispositivos», señaló Mandiant en un análisis publicado esta semana. La firma de inteligencia de amenazas propiedad de Google está monitoreando las actividades del actor bajo el alias UNC5221.

Los ataques emplean una cadena de exploits que incluye una vulnerabilidad de bypass de autenticación (CVE-2023-46805) y una vulnerabilidad de inyección de código (CVE-2024-21887) para tomar el control de las instancias susceptibles.

Volexity, que atribuyó la actividad a un presunto actor de espionaje chino llamado UTA0178, indicó que las dos fallas fueron utilizadas para obtener acceso inicial, desplegar capas de seguridad web, establecer accesos traseros en archivos legítimos, capturar credenciales y datos de configuración, y avanzar más en el entorno de la víctima.

De acuerdo con Ivanti, las intrusiones afectaron a menos de 10 clientes, sugiriendo que podría tratarse de una campaña altamente dirigida. Se espera que los parches para las dos vulnerabilidades (colloquialmente denominadas ConnectAround) estén disponibles en la semana del 22 de enero.

El análisis de Mandiant de los ataques ha revelado la existencia de cinco familias diferentes de software malicioso personalizado, además de la inserción de código malicioso en archivos legítimos dentro de ICS y la utilización de otras herramientas legítimas como BusyBox y PySoxy para facilitar la actividad posterior.

> *«Dado que ciertas secciones del dispositivo son de solo lectura, UNC5221 utilizó un script en Perl (sessionserver.pl) para remontar el sistema de archivos como de*

> *lectura/escritura y permitir la implementación de THINSPOOL, un script de instalación que escribe el web shell LIGHTWIRE en un archivo legítimo de Connect Secure, junto con otras herramientas adicionales»*, detalló la empresa.

LIGHTWIRE es uno de los dos web shells, siendo el otro WIREFIRE; ambos son *«puntos de apoyo ligeros»* diseñados para asegurar un acceso remoto persistente a dispositivos comprometidos. Mientras que LIGHTWIRE está desarrollado en Perl CGI, WIREFIRE se implementa en Python.

En estos ataques también se emplea un ladrón de credenciales basado en JavaScript denominado WARPWIRE, y una puerta trasera pasiva llamada ZIPLINE, capaz de descargar/subir archivos, establecer un shell inverso, crear un servidor proxy y configurar un servidor de túneles para dirigir el tráfico entre múltiples puntos finales.

> *«Esto indica que no se trata de ataques oportunísticos, y UNC5221 tenía la intención de mantener su presencia en un conjunto específico de objetivos de alta prioridad que comprometió después de que se lanzara inevitablemente un parche»,* agregó Mandiant.

Aunque UNC5221 no ha sido vinculado anteriormente a ningún grupo conocido o país en particular, el hecho de atacar la infraestructura perimetral mediante la explotación de vulnerabilidades de día cero y el uso de infraestructura comprometida de comando y control (C2) para eludir la detección presenta todas las características de una amenaza persistente avanzada (APT).

> *«La actividad de UNC5221 demuestra que explotar y mantenerse en el borde de las redes sigue siendo un objetivo viable y atractivo para actores de espionaje»,* concluyó Mandiant.