La Corporación MITRE ha informado que fue objeto de un ataque cibernético perpetrado por un estado-nación, el cual aprovechó dos vulnerabilidades recién descubiertas en los dispositivos Ivanti Connect Secure a partir de enero de 2024.

Esta intrusión condujo al compromiso de su Entorno de Experimentación, Investigación y Virtualización en Red (NERVE), una red de investigación y prototipado sin clasificación.

Según Lex Crumpton, un investigador en operaciones cibernéticas defensivas de la organización sin fines de lucro, el adversario desconocido llevó a cabo un reconocimiento de las redes, explotó una de las Redes Privadas Virtuales (VPN) a través de dos vulnerabilidades recién descubiertas en Ivanti Connect Secure, y logró evadir la autenticación de múltiples factores mediante la suplantación de sesiones.

Este ataque involucró la explotación de dos vulnerabilidades conocidas como CVE-2023-46805 (con una puntuación CVSS de 8.2) y CVE-2024-21887 (con una puntuación CVSS de 9.1), las cuales podrían ser utilizadas por actores maliciosos para eludir la autenticación y ejecutar comandos arbitrarios en los sistemas infectados.

Después de obtener acceso inicial, los atacantes se movieron lateralmente y comprometieron la infraestructura VMware utilizando una cuenta de administrador comprometida, lo que finalmente les permitió desplegar puertas traseras y shells web para mantener su acceso y robar credenciales.

> *«NERVE es una red colaborativa no clasificada que proporciona recursos de almacenamiento, computación y redes. Según nuestra investigación hasta la fecha, no hay indicios de que la red empresarial principal de MITRE o los sistemas de sus socios se hayan visto afectados por este incidente»*, explicó MITRE.

La organización afirmó que ha tomado medidas para contener el incidente, además de realizar esfuerzos de respuesta y recuperación, así como análisis forense para determinar el alcance del compromiso.

Se ha atribuido la explotación inicial de estas vulnerabilidades a un grupo identificado por la empresa de ciberseguridad Volexity como UTA0178, un actor probablemente respaldado por un estado-nación con vínculos a China. Desde entonces, varios otros grupos de piratería, también vinculados a China, se han sumado a la explotación de estas vulnerabilidades, según Mandiant.

> *«Ninguna organización está exenta de este tipo de ataques cibernéticos, ni siquiera aquellas que se esfuerzan por mantener los más altos estándares de seguridad cibernética,»* afirmó Jason Providakes, presidente y CEO de MITRE.
>
> *«Estamos compartiendo este incidente de manera oportuna debido a nuestro compromiso de operar en beneficio del interés público y de promover las mejores prácticas que mejoren la seguridad empresarial, así como las medidas necesarias para fortalecer la postura de defensa cibernética actual de la industria.»*