Una vulnerabilidad de solicitud falsificada del lado del servidor (SSRF) recientemente revelada, que afecta a los productos Ivanti Connect Secure y Policy Secure, está siendo objeto de una explotación generalizada.

Según la Fundación Shadowserver, se han detectado intentos de explotación provenientes de más de 170 direcciones IP únicas, buscando establecer un shell inverso, entre otros objetivos.

Estos ataques aprovechan la CVE-2024-21893 (puntuación CVSS: 8.2), una falla de SSRF en el componente SAML de Ivanti Connect Secure, Policy Secure y Neurons for ZTA, que permite a un atacante acceder a recursos restringidos sin autenticación.

Ivanti había informado previamente que la vulnerabilidad se había utilizado en ataques dirigidos a un *«número limitado de clientes»,* pero advirtió que la situación podría cambiar después de la divulgación pública.

Eso es exactamente lo que parece haber sucedido, especialmente después de la publicación de un exploit de prueba de concepto (PoC) por parte de la firma de ciberseguridad Rapid7 la semana pasada.

El PoC implica la creación de una cadena de exploits que combina la CVE-2024-21893 con la CVE-2024-21887, una falla de inyección de comandos previamente parchada, para lograr la ejecución remota de código sin autenticación.

Es relevante señalar aquí que la CVE-2024-21893 es un alias para la CVE-2023-36661 (puntuación CVSS: 7.5), una vulnerabilidad de SSRF presente en la biblioteca XMLTooling de código abierto Shibboleth. Esta fue corregida por los mantenedores en junio de 2023 con el lanzamiento de la versión 3.2.4.

El investigador de seguridad Will Dormann también destacó otros componentes de código abierto desactualizados utilizados por los dispositivos VPN de Ivanti, como curl 7.19.7, openssl 1.0.2n-fips, perl 5.6.1, psql 9.6.14, cabextract 0.5, ssh 5.3p1 y unzip 6.00, lo que

abre la puerta a más ataques.

Este desarrollo se produce mientras los actores de amenazas han encontrado una manera de eludir la mitigación inicial de Ivanti, lo que llevó a la empresa con sede en Utah a lanzar un segundo archivo de mitigación. A partir del 1 de febrero de 2024, ha comenzado a lanzar parches oficiales para abordar todas las vulnerabilidades.

La semana pasada, Mandiant, propiedad de Google, reveló que varios actores de amenazas están aprovechando la CVE-2023-46805 y la CVE-2024-21887 para implementar una variedad de shells web personalizados rastreados como BUSHWALK, CHAINLINE, FRAMESTING y LIGHTWIRE.

Palo Alto Networks Unit 42 informó que observó 28,474 instancias expuestas de Ivanti Connect Secure y Policy Secure en 145 países entre el 26 y el 30 de enero de 2024, con 610 instancias comprometidas detectadas en 44 países hasta el 23 de enero de 2024.

La explotación continua de las fallas de Ivanti también ha llevado a la Unión Europea, junto con CERT-EU, ENISA y Europol, a emitir un aviso conjunto instando a las organizaciones en el bloque a seguir las indicaciones proporcionadas por el proveedor para mitigar posibles riesgos.