Vulnerabilidades de alta severidad en productos de Ivanti

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de la Agencia de Ciberseguridad Vasca como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de la Agencia de Ciberseguridad Vasca. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

1. Resumen ejecutivo

Ivanti ha publicado un aviso de seguridad para tratar **dos vulnerabilidades** de **severidad alta**, CVE-2024-21888 de escalada de privilegios y CVE-2024-21893 de Server-Side Request Forgery (SSRF). Estos errores afectan a los productos **Ivanti Policy Secure Gateways**, **Ivanti Connect Secure** e **Ivanti Neurons for ZTA,** que, de ser explotados, podrían suponer una amenaza de gravedad crítica para varios productos de Ivanti con un impacto en la confidencialidad de los sistemas que se vean afectados.

Por el momento, se han hecho publicas medidas de mitigación por parte del fabricante a la espera de las actualizaciones de seguridad que resuelvan las vulnerabilidades.

2. Recursos afectados

- Ivanti Policy Secure 9.x, 22.x.
- Ivanti Connect Secure 9.x, 22.x.
- Ivanti Neurons for ZTA.

3. Análisis técnico

Los detalles de las vulnerabilidades tratadas en este aviso son los siguientes:

CVE-2024-21888: vulnerabilidad de escalada de privilegios en el componente web de Ivanti Connect Secure (9.x, 22.x) e Ivanti Policy Secure (9.x, 22.x) permite a un usuario elevar privilegios a privilegios de administrador.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.8**

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Bajos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-21893: vulnerabilidad de tipo Server-Side Request Forgery (SSRF) (falsificación de solicitudes del lado del servidor) en el componente SAML de Ivanti Connect Secure (9.x, 22.x) e Ivanti Policy Secure (9.x, 22.x) e Ivanti Neurons for ZTA permite a un atacante acceder a ciertos recursos restringidos. sin autenticación.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 918: Server-Side Request Forgery (SSRF)

CVSS Base: **8.2**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad:** Baja
- **Disponibilidad:** Ninguna

4. Mitigación / Solución

Como es habitual, para prevenir esta y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Desde Ivanti se informa, que los parches están disponibles para su descarga a través del portal de descarga estándar para Ivanti Connect Secure para las versiones (9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2 y 22.5R1. 1) y ZTA versión 22.6R1.3.

Por otra parte, el fabricante enfatiza que es fundamental que los clientes tomen medidas de inmediato para asegurarse de estar completamente protegidos. Para ello los clientes pueden consultar el documento KB Article para saber cómo aplicar las medidas de mitigación.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-21888.
- CVE-2024-21893.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY