Vulnerabilidades en Ivanti Connect Secure e Ivanti Policy Secure

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

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 vulnerabilidades de **severidad alta** en los productos **Ivanti Connect Secure (ICS)** e **Ivanti Policy Secure**, con los identificadores CVE-2024-21894, CVE-2024-22052, CVE-2024-22053. También se corrige un fallo de severidad media, CVE-2024-22023. Todos estos errores tienen **impacto en la disponibilidad** de los sistemas que se vean afectados.

Por otra parte, desde Ivanti se informa de no tener constancia de la explotación de estas vulnerabilidades.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir esta y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Recursos afectados

- Ivanti Connect Secure versiones 9.x, 22.x.
- Ivanti Policy Secure versiones 22.4R1.2, 22.5R1.3, 22.6R1.2, 9.1R16.4, 9.1R17.4 y 9.1R18.5.

3. Análisis técnico

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

CVE-2024-21894: vulnerabilidad de desbordamiento del heap en el componente IPSec de Ivanti Connect Secure y Ivanti Policy Secure que permite que un usuario malicioso, no autenticado, envíe solicitudes especialmente diseñadas para hacer que el servicio se bloquee, lo que provoca un ataque DoS. En ciertas condiciones, esto podría conducir a la ejecución de código arbitrario.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE 122: Heap-based Buffer Overflow

CVSS Base: **8.2**

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

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

CVE-2024-22053: vulnerabilidad de desbordamiento del heap en el componente IPSec de Ivanti Connect Secure y Ivanti Policy Secure que permite que un usuario malicioso, no autenticado, envíe solicitudes especialmente diseñadas para hacer que el servicio se bloquee, lo que provoca un ataque DoS. En ciertas condiciones, esto podría conducir a la ejecución de código arbitrario.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE 122: Heap-based Buffer Overflow

CVSS Base: **8.2**

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

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

CVE-2024-22052: vulnerabilidad de referencia nula de puntero en el componente IPSec de Ivanti Connect Secure 9.x, 22.x e Ivanti Policy Secure que permite que un usuario malicioso no autenticado envíe solicitudes especialmente diseñadas con el fin de hacer que el servicio se bloquee, lo que provoca un ataque de denegación de servicio (DoS).

La métrica de evaluación de las vulnerabilidades se compone de:

CWE 476: NULL Pointer Dereference

CVSS Base: **7.5**

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

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

4. Mitigación / Solución

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

Para solucionar y aplicar las correcciones oportunas a estas vulnerabilidades, desde Ivanti se recomienda a sus clientes que actualicen los productos afectados a una versión corregida, las cuales se pueden consultar desde el siguiente enlace.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-21894.
- CVE-2024-22052.
- CVE-2024-22053.
- CVE-2024-22023.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY