Vulnerabilidades críticas 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 avisos de seguridad para tratar **2 vulnerabilidades** de **severidad crítica,** CVE-2023-46808 de **escritura remota de archivos autenticada** y CVE-2023-41724 de **ejecución remota de código** que afectan a los productos **Ivanti Neurons para ITSM** e **Ivanti Standalone Sentry,** respectivamente. Los fallos suponen una amenaza de gravedad crítica con impacto en la confidencialidad, integridad y disponibilidad de los sistemas que se vean afectados.

Por otra parte, desde Ivanti se informa que no hay evidencias que indiquen que estas vulnerabilidades hayan sido explotadas activamente.

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 Neurons para ITSM 2023.1, 2023.2, 2023.3
- Ivanti Standalone Sentry 9.17.0, 9.18.0 y 9.19.0, (versiones anteriores también están en riesgo).

3. Análisis técnico

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

CVE-2023-46808: vulnerabilidad que podría posibilitar a agentes malintencionados escribir archivos en directorios sensibles y, por consiguiente, llevar a cabo la ejecución de comandos en el contexto del usuario de la aplicación web. Para llevar a cabo esta acción, el individuo malintencionado debe haber sido autenticado previamente por el sistema.

Esta vulnerabilidad afecta a todas las versiones compatibles de Ivanti Neurons para ITSM (2023.3, 2023.2 y 2023.1).

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **9.9**

CVSS:3.0/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-2023-41724: vulnerabilidad de ejecución remota de código que permitiría a un actor malintencionado, que se encuentre dentro de la misma red física o lógica, la explotación de comandos arbitrarios en el sistema operativo del dispositivo.

La vulnerabilidad afecta a todas las versiones compatibles de **Ivanti Standalone Sentry** (9.17.0, 9.18.0 y 9.19.0), así como a versiones antiguas y no compatibles (anteriores a la versión 9.17.0).

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **9.6**

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

- **Vector de ataque**: Adyacente
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**

- **Integridad: Alta**
- **Disponibilidad: Alta**

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, en el caso de la vulnerabilidad CVE-2023-46808, de la existencia de un parche para todas las versiones compatibles de Ivanti Neurons para ITSM (2023.3, 2023.2 y 2023.1).

En el caso de la vulnerabilidad CVE-2023-41724, el equipo de Ivanti informa de la disponibilidad de un parche aplicable a todas las versiones compatibles de Ivanti Standalone Sentry 9.17.0, 9.18.0 y 9.19.0.

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

- Avisos de seguridad.
- CVE-2023-46808.
- CVE-2023-41724.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY