Vulnerabilidades críticas en Ivanti Avalanche

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

TABLA DE CONTENIDO

1. Resumen ejecutivo 3
2. Recursos afectados 4
3. Análisis técnico 5
4. Mitigación / Solución 13
5. Referencias Adicionales 14

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 un total de 28 vulnerabilidades que afectan a **Ivanti Avalanche** 6.3.1 y versiones superiores, estas vulnerabilidades han sido fijadas en la versión 6.4.3 Avalanche On-Premise.

De las vulnerabilidades tratadas **2** son de **severidad crítica** siendo sus identificadores CVE-2024-24996 y CVE-2024-29204 y **17** de **severidad alta** cuyos identificadores son CVE-2024-27976, CVE-2024-27975, CVE-2024-25000, CVE-2024-24999, CVE-2024-24998, CVE-2024-24997, CVE-2024-24995, CVE-2024-24994, CVE-2024-24993, CVE-2024-24992, CVE-2024-23535, CVE-2024-23534, CVE-2024-22061, CVE-2024-23532, CVE-2024-23531, CVE-2024-27984, CVE-2024-27977.

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 Avalanche 6.3.1 y versiones superiores.

3. Análisis técnico

Los detalles de la vulnerabilidad tratada en este aviso son los siguientes:

CVE-2024-24996: vulnerabilidad de desbordamiento de Heap en el componente **WLInfoRailService** de Ivanti Avalanche en versiones anteriores a la versión 6.4.3. La explotación de esta vulnerabilidad permitiría a un atacante remoto la ejecución de comandos arbitrarios.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **9.8**

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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

CVE-2024-29204: vulnerabilidad de desbordamiento de Heap en el componente WLAvalancheService en versiones de Ivanti Avalanche anteriores a la versión 6.4.3. La explotación de esta vulnerabilidad podría permitir la ejecución de comandos arbitrarios por parte de un atacante no autenticado.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **9.8**

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

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

CVE-2024-23534: vulnerabilidad de carga de archivos no restringida en el componente web de Ivanti Avalanche antes de la versión 6.4.3 permitiría a un atacante remoto autenticado ejecutar comandos arbitrarios como SYSTEM.

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:U/C:H/I:H/A:H

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

CVE-2024-23535: vulnerabilidad de tipo Path Traversal en el componente web de Ivanti Avalanche antes de la versión 6.4.3 permite a un atacante remoto autenticado ejecutar comandos arbitrarios como SYSTEM.

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:U/C:H/I:H/A:H

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

CVE-2024-24992: vulnerabilidad de tipo Path Traversal en el componente web de Ivanti Avalanche antes de la versión 6.4.3 permite a un atacante remoto autenticado ejecutar comandos arbitrarios como SYSTEM.

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:U/C:H/I:H/A:H

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

- **Disponibilidad: Alta**

CVE-2024-24993: vulnerabilidad de tipo condición de carrera (TOCTOU) en el componente web de Ivanti Avalanche antes de la versión 6.4.3 permite a un atacante remoto autenticado ejecutar comandos arbitrarios como SYSTEM.

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:U/C:H/I:H/A:H

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

CVE-2024-24994: vulnerabilidad de tipo Path Traversal en el componente web de Ivanti Avalanche antes de la versión 6.4.3 permite a un atacante remoto autenticado ejecutar comandos arbitrarios como SYSTEM.

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:U/C:H/I:H/A:H

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

CVE-2024-24995: vulnerabilidad de condición de carrera (TOCTOU) en el componente web de Ivanti Avalanche antes de la versión 6.4.3 permite a un atacante remoto autenticado ejecutar comandos arbitrarios como SYSTEM.

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:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**

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

CVE-2024-24997: vulnerabilidad de tipo Path Traversal en el componente web de Ivanti Avalanche antes de la versión 6.4.3 permite que un atacante remoto autenticado ejecute comandos arbitrarios como SYSTEM.

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:U/C:H/I:H/A:H

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

CVE-2024-24998: vulnerabilidad de tipo Path Traversal en el componente web de Ivanti Avalanche antes de la versión 6.4.3 permite que un atacante remoto autenticado ejecute comandos arbitrarios como SYSTEM.

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:U/C:H/I:H/A:H

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

CVE-2024-24999: vulnerabilidad de tipo Path Traversal en el componente web de Ivanti Avalanche antes de la versión 6.4.3 permite que un atacante remoto autenticado ejecute comandos arbitrarios como SYSTEM.

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:U/C:H/I:H/A:H

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

CVE-2024-25000: vulnerabilidad de tipo Path Traversal en el componente web de Ivanti Avalanche antes de la versión 6.4.3 permite que un atacante remoto autenticado ejecute comandos arbitrarios como SYSTEM.

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:U/C:H/I:H/A:H

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

CVE-2024-27975: vulnerabilidad de ejecución remota de código Use-After-Free en Ivanti Avalanche WLAvalancheService.

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:U/C:H/I:H/A:H

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

- **Disponibilidad: Alta**

CVE-2024-27976: vulnerabilidad de tipo Path Traversal en el componente web de Ivanti Avalanche antes de la versión 6.4.3 permite que un atacante remoto autenticado ejecute comandos arbitrarios como SYSTEM.

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:U/C:H/I:H/A:H

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

CVE-2024-22061: vulnerabilidad de tipo Heap Overflow en WLInfoRailService antes de la versión 6.4.3 permite que un atacante remoto no autenticado ejecute comandos arbitrarios.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.1**

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

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

CVE-2024-23531: vulnerabilidad de desbordamiento de enteros en el componente WLInfoRailService de Ivanti Avalanche antes de la versión 6.4.3 permite a un atacante remoto no autenticado realizar ataques de denegación de servicio. En ciertas condiciones poco comunes, esto también podría llevar a la lectura de contenido de la memoria.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.5**

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

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

CVE-2024-23532: vulnerabilidad de lectura fuera de límites en el componente WLAvalancheService de Ivanti Avalanche antes de la versión 6.4.3 permite a un atacante remoto autenticado realizar ataques de denegación de servicio. En ciertas condiciones, esto también podría conducir a la ejecución remota de código.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.5**

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

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

CVE-2024-27977: vulnerabilidad de tipo Path Traversal en el componente web de Ivanti Avalanche antes de la versión 6.4.3 permite que un atacante remoto autenticado elimine archivos arbitrarios, lo que conduce a una Denegación de Servicio.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.1**

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

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad:** Ninguno
- **Integridad:** Bajo

- **Disponibilidad: Alta**

CVE-2024-27984: vulnerabilidad de tipo Path Traversal en el componente web de Ivanti Avalanche antes de la versión 6.4.3 permite que un atacante remoto autenticado elimine un tipo específico de archivos y/o provoque una denegación de servicio.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.1**

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

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad:** Ninguno
- **Integridad:** Ninguno
- **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, que es altamente recomendable descargar el instalador de Avalanche y actualizar a la última versión de Avalanche 6.4.3.

5. Referencias Adicionales

- Avisos de seguridad.
- CVE-2024-24996.
- CVE-2024-29204.
- CVE-2024-27976, CVE-2024-27975, CVE-2024-25000, CVE-2024-24999, CVE-2024-24998, CVE-2024-24997, CVE-2024-24995, CVE-2024-24994, CVE-2024-24993, CVE-2024-24992, CVE-2024-23535, CVE-2024-23534, CVE-2024-22061, CVE-2024-23532, CVE-2024-23531, CVE-2024-27984, CVE-2024-27977.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY