Vulnerabilidades en productos de Atlassian

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 el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC 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 BCSC 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 BCSC. 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

Atlassian ha publicado su actualización de seguridad mensual donde se tratan múltiples vulnerabilidades, una de severidad crítica y varias alta, las cuales afectan a los productos **Bamboo Data Center and Server, Bitbucket Data Center and Server** y **Confluence Data Center and Server**.

Las vulnerabilidades nuevas más relevantes abordadas tienen los identificadores CVE-2024-1597, CVE-2024-21634 y CVE-2024-21677. La explotación de todas ellas representa una amenaza de alta gravedad para la disponibilidad de los sistemas que se vean afectados. En el caso de la primera también se ven comprometidas la confidencialidad y la integridad.

En cuanto a la vulnerabilidad CVE-2024-1597, hay que destacar que es un **fallo de severidad crítica** en una dependencia de Bamboo que no es de Atlassian. Sin embargo, la aplicación de Atlassian de la dependencia presenta un riesgo menor evaluado, razón por la cual se ha divulgado la vulnerabilidad en el Boletín de Seguridad mensual de Atlassian en lugar de un Aviso de Seguridad Crítico.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir estas 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

- Confluence Data Server.
- Bamboo Data Center y Server.
- Bitbucket Data Center y Server.

3. Análisis técnico

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

CVE-2024-1597: es una vulnerabilidad crítica de inyección SQL en Bamboo Data Center y Server, podría permitir a un atacante no autenticado exponer activos de su entorno susceptibles de explotación, lo que tiene un alto impacto en la confidencialidad, un alto impacto en la integridad, un alto impacto en la disponibilidad y no requiere la interacción del usuario.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **10**

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

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

CVE-2024-21677: vulnerabilidad de Path Transversal de gravedad alta afecta al Confluence Data Center y podría permitir a un atacante no autenticado explotar una vulnerabilidad indefinible que tiene un alto impacto en la confidencialidad, un alto impacto en la integridad, un alto impacto en la disponibilidad y requiere la interacción del usuario.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.3**

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

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

CVE-2024-21634: vulnerabilidad de denegación de servicio (DoS) alta que afecta a Bamboo Data Center y a Bitbucket Data Center y Server, la cual podría permitir a un atacante no autenticado exponer activos de su entorno susceptibles de explotación que no tienen ningún impacto en la confidencialidad, ningún impacto en la integridad, un alto impacto en la disponibilidad y no requiere la interacción del usuario.

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:N/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ninguno**
- **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 corregir todas las vulnerabilidades, Atlassian recomienda aplicar parches a sus instancias para actualizarlas a la última versión. Si no se puede hacer, se deben aplicar las actualizaciones para la versión mínima de corrección que se indican a continuación:

- **Bamboo Data Center y Server**: Atlassian recomienda actualizar a la última versión, si no, actualizar la instancia a una de las versiones fijas soportadas especificadas.

- **Confluence Data Center y Server**: Atlassian recomienda actualizar a la última versión. Si no, actualizar la instancia a una de las versiones fijas compatibles especificadas.

- **Bitbucket Data Center y Server**: Atlassian recomienda actualizar a la última versión, si no, actualizar la instancia a una de las versiones fijas soportadas especificadas.

5. Referencias Adicionales

- Actualización de seguridad mensual.
- CVE-2024-1597.
- CVE-2024-21634.
- CVE-2024-21677.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY