Vulnerabilidades de alta severidad 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 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

Atlassian ha publicado su actualización de seguridad mensual donde se tratan múltiples vulnerabilidades de **severidad alta** que afectan a los productos **Bamboo Data Center y Server, Confluence Data Center y Server, Jira Software Data Center y Server, Jira Service Management Data Center y Server**.

La explotación de la mayoría de ellas representa una amenaza de alta gravedad para la **confidencialidad** de los sistemas que se vean afectados.

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

- **Bamboo Data Center y Server**, versiones 9.6.0, 9.5.0 a 9.5.2, 9.4.0 a 9.4.3, 9.3.0 a 9.3.6, 9.2.0 a 9.2.12 (LTS), 9.1.0 a 9.1.3, 9.0.0 a 9.0.4, 8.2.0 a 8.2.9 y cualquier versión anterior.
- **Confluence Data Center y Server**, versiones 8.7.0, 8.6.0 a 8.6.2, 8.5.0 a 8.5.6 (LTS), 8.4.0 a 8.4.5, 8.3.0 a 8.3.4, 8.2.0 a 8.2.3, 8.1.0 a 8.1.4, 8.0.0 a 8.0.4, 7.20.0 a 7.20.3, 7.19.0 al 7.19.19 (LTS), 7.18.0 a 7.18.3, 7.17.0 a 7.17.5 y cualquier versión anterior.
- **Jira Software Data Center y Server**, versiones 9.14.0 a 9.14.1, 9.13.0 a 9.13.1, 9.12.0 a 9.12.5 LTS, 9.11.0 a 9.11.3, 9.10.0 a 9.10.2, 9.9.0 a 9.9.2, 9.8.0 a 9.8.2, 9.7.0 a 9.7.2, 9.6.0, 9.5.0 a 9.5.1, 9.4.0 a 9.4.17 LTS, 9.3.0 a 9.3.3, 9.2.0 a 9.2.1, 9.1.0 a 9.1.1, 9.0.0 y cualquier versión anterior.
- **Jira Service Management Data Center y Server**, versiones de 5.12.0 a 5.12.5 (LTS), de 5.11.0 a 5.11.3, de 5.10.0 a 5.10.2, de 5.9.0 a 5.9.2, de 5.8.0 a 5.8.2, de 5.7.0 a 5.7.2, de 5.6.0 a 5.6.2, de 5.5.0 a 5.5.1, de 5.4.0 a 5.4.18 (LTS) y cualquier versión anterior.

3. Análisis técnico

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

CVE-2024-22257: vulnerabilidad de dependencia de alta gravedad en *org.springframework.security:spring-security-core,* que se introdujo en las versiones 8.2.1, 9.0.0, 9.1.0, 9.2.1, 9.3.0, 9.4.0, 9.5.0 y 9.6.0 de Bamboo Data Center y Server. El error permite que un atacante no autenticado exponga activos en entornos susceptibles de explotación, lo que tiene un alto impacto en la confidencialidad, un bajo impacto en la integridad, ningún impacto en la disponibilidad y no requiere interacción del usuario.

La métrica de evaluación de la vulnerabilidad se compone de:

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: Ninguno**
- **Interacción del usuario: Ninguno**
- **Ámbito de aplicación:** Sin cambios
- **Confidencialidad: Alta**
- **Integridad:** Baja
- **Disponibilidad:** Ninguna

CVE-2024-22259: vulnerabilidad de dependencia en *org.springframework:spring-web,* de alta gravedad, que se introdujo en las versiones 8.2.1, 9.0.0, 9.1.0, 9.2.1, 9.3.0, 9.4.0, 9.5.0 y 9.6.0 de Bamboo Data Center y Server. El fallo permite que un atacante no autenticado exponga activos en entornos susceptibles de explotación, lo que tiene un alto impacto en la confidencialidad, un alto impacto en la integridad, ningún impacto en la disponibilidad y requiere la interacción del usuario.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.1**

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

- **Vector de Ataque: Red**
- **Complejidad del ataque: Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción del usuario:** Requerida
- **Ámbito de aplicación:** Sin cambios
- **Confidencialidad: Alta**

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

CVE-2024-22243: vulnerabilidad de dependencia en *org.springframework:spring-web*, de gravedad alta, que se introdujo en las versiones 8.2.1, 9.0.0, 9.1.0, 9.2.1, 9.3.0, 9.4.0 y 9.5.0 de Bamboo Data Center and Server. El error permite que un atacante no autenticado exponga activos en entornos susceptibles de explotación, lo que tiene un alto impacto en la confidencialidad, un alto impacto en la integridad, ningún impacto en la disponibilidad y requiere la interacción del usuario.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.1**

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

- **Vector de Ataque: Red**
- **Complejidad del ataque: Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción del usuario:** Requerida
- **Ámbito de aplicación:** Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad:** Ninguna

CVE-2024-21634: vulnerabilidad de denegación de servicio DoS producida por la dependencia *software.amazon.ion:ion-java*, de alta gravedad, que se introdujo en las versiones 5.6 de Confluence Data Center y Server. La vulnerabilidad permite que un atacante no autenticado exponga activos en entornos susceptibles de explotación, lo que no tiene ningún impacto en la confidencialidad, ningún impacto en la integridad, un alto impacto en la disponibilidad y no requiere interacción del usuario.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 770: Allocation of Resources Without Limits or Throttling

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 del usuario: Ninguna**
- **Ámbito de aplicación:** Sin cambios
- **Confidencialidad:** Ninguna
- **Integridad:** Ninguna

- **Disponibilidad: Alta**

CVE-2023-1370: vulnerabilidad de denegación de servicio DoS producida por la dependencia *net.minidev:json-smart,* de alta gravedad, que se introdujo en las versiones 8.20.0, 9.0.0, 9.1.0, 9.2.0, 9.3.0, 9.4.0, 9.5.0, 9.6.0, 9.7. 0, 9.8.0, 9.9.0, 9.10.0, 9.11.0 y 9.12.0 de Jira Software Data Center y Server. El fallo permite que un atacante no autenticado exponga activos en entornos susceptibles de explotación, lo que no tiene ningún impacto en la confidencialidad, ningún impacto en la integridad, un alto impacto en la disponibilidad y no requiere interacción del usuario.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 674: Allocation of Resources Without Limits or Throttling

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 del usuario: Ninguna**
- **Ámbito de aplicación:** Sin cambios
- **Confidencialidad:** Ninguna
- **Integridad:** Ninguna
- **Disponibilidad: Alta**

CVE-2023-52428: vulnerabilidad de denegación de servicio DoS producida por la dependencia *com.nimbusds:nimbus-jose-jwt* que se introdujo en las versiones 5.4, 5.11 y 5.12 de Jira Service Management Data Center and Server. Los detalles de la vulnerabilidad aún no han sido difundidos a fecha de publicación de este aviso.

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**: actualizar a la versión recomendada 9.6.1 LTS (sólo centro de datos), 9.5.3 (sólo centro de datos) y 9.2.13 (LTS).
- **Confluence Data Center y Server**: actualizar a una versión mínima de corrección 8.9.0 (sólo centro de datos), 8.8.0 (sólo centro de datos), de 8.7.1 a 8.7.2 (sólo centro de datos), de 8.5.7 a 8.5.8 (LTS) y de 19.7.20 a 19.7.21 (LTS).
- **Jira Software Data Center y Server**: actualizar a una versión mínima de corrección 9.15.0 (sólo centro de datos), de 9.12.6 a 9.12.7 (LTS) y de 9.4.18 a 9.4.20 (LTS).
- **Jira Service Management Data Center y Server**: actualizar a una versión mínima de corrección 5.15.0, 5.14.0, 5.14.1 (sólo centro de datos), 5.12.6 (LTS) recomendado y 5.4.19 (LTS).

5. Referencias Adicionales

- Actualización de seguridad mensual.
- Aviso de seguridad.
- CVE-2024-22257.
- CVE-2024-22259.
- CVE-2024-22243.
- CVE-2023-1370.
- CVE-2023-52428.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY