Basque CyberSecurity Centre

Vulnerabilidad crítica en productos Atlassian

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

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 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.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Resumen ejecutivo

Atlassian ha publicado un aviso de seguridad en donde se trata la **vulnerabilidad crítica** de ejecución remota de código, reportada con anterioridad en Apache ActiveMQ, cuyo identificador es CVE-2023-46604, que afecta a los productos Bamboo Data Center y Bamboo Server. El error, de ser explotado, produce un impacto de alta gravedad en la integridad y disponibilidad de los sistemas que se vean afectados.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera el fallo destacado. 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. Productos afectados

- Todas las versiones de Bamboo Data Center y Bamboo Server.

2. Análisis técnico

CVE-2023-46604: vulnerabilidad de ejecución remota de código que afecta a la librería Apache ActiveMQ, que es utlizada por Bamboo como parte de sus servicios principales. La vulnerabilidad puede permitir que un atacante remoto con acceso a la red ejecute comandos de shell arbitrarios al manipular tipos de clases serializadas en el protocolo OpenWire y que se instancie cualquier clase en la ruta de clases.

La métrica de evaluación de la vulnerabilidad anteriormente descrita se componen de:

CVSS Base: **10.0**

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

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

3. 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 esta vulnerabilidad, desde Atlassian se recomienda actualizar a las versiones corregidas de Bamboo Data Center y Bamboo Server, 9.2.7 o posterior, 9.3.5 o posterior y 9.4.1 o posterior, disponibles desde el centro de descargas.

Adicionalmente, se ofrecen medidas de mitigación provisionales en el caso de no poder actualizar, que consisten en:

Asegurarse que el servidor Bamboo esté detrás de un firewall/VPC y solo permita conexiones a los puertos del broker ActiveMQ desde fuentes de confianza. Los puertos predeterminados para ActiveMQ son:

- TCP/54663
- TCP/54664
- TCP/54665

Estos puertos pueden ser personalizados. Para ello se puede consultar la sección de preguntas frecuentes (FAQ) para obtener información adicional.

4. Referencias Adicionales

- Aviso de seguridad.
- CVE-2023-46604.


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA