Basque CyberSecurity Centre

Vulnerabilidades críticas en Apache Airflow y Apache bRPC

BCSC-AVISOS

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 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.

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. Aviso de seguridad

Apache ha actualizado el estado de dos avisos de seguridad, aviso para Apache Airflow y aviso para Apache bPRC, que hacen referencia a dos vulnerabilidades de severidad crítica para los productos Apache Airflow y Apache bRPC. Los identificadores de estos fallos son CVE-2023-25754 y CVE-2023-31039 respectivamente. Su explotación exitosa, en ambos casos, supone un impacto de alta gravedad en la confidencialidad, integridad y disponibilidad de los sistemas afectados.

El fabricante ya ha publicado las actualizaciones correspondientes corrigiendo de esta manera los fallos destacados, por lo que, para prevenir estas y otras vulnerabilidades, se recomienda mantener siempre actualizados los sistemas y aplicaciones.

2. Recursos afectados

- Apache Airflow en las versiones anteriores a la 2.6.0.
- Apache bRPC en versiones anteriores a la 1.5.0.

3. Análisis técnico

Los detalles de las vulnerabilidades aboradas con estas actualizaciones son:

CVE-2023-25754: vulnerabilidad de error de cambio de contexto de privilegio en Apache Software Foundation Apache Airflow. Este problema afecta a Apache Airflow en las versiones anteriores a la 2.6.0.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 270: Privilege Context Switching Error

CVSS Base: 9.8

CVSS:3.1/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: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-31039: vulnerabilidad en Apache bRPC para versiones anteriores a la 1.5.0 en todas las plataformas que permite a los atacantes ejecutar código arbitrario a través de *ServerOptions::pid_file*. Un atacante que pueda influir en el parámetro *pid_file* de *ServerOptions* con el que se inicia el servidor bRPC puede ejecutar código arbitrario con los permisos del proceso bRPC.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 502: Deserialization of Untrusted Data

CVSS Base: 9.8

CVSS:3.1/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: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

4. Mitigación / Solución

Para la mitigación de estas vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para la vulnerabilidad CVE-2023-25754 que afecta a Apache Airflow se recomienda:

- Actualizar a la versión de Apache Airflow 2.6.0, disponible desde el siguiente enlace.

En el caso de la vulnerabilidad CVE-2023-31039 que afecta a Apache bPRC se recomienda:

- Actualizar a bRPC en la versión 1.5.0 o superior, cuyo enlace de descarga es versión 1.5.0.
- Si se está utilizando una versión anterior de bRPC y es difícil de actualizar, se puede aplicar el siguiente parche.

5. Referencias Adicionales

- Aviso para Apache Airflow.
- Aviso para Apache bPRC.
- CVE-2023-25754.
- CVE-2023-31039.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA