Basque CyberSecurity Centre

Vulnerabilidades en VMware Aria Operations

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

VMware ha publicado un aviso de seguridad que aborda cuatro vulnerabilidades identificadas como CVE-2023-20877, CVE-2023-20878, CVE-2023-20879, CVE-2023-20880. La primera de estas vulnerabilidades es un fallo de escalada de privilegios de alta gravedad, lo que la convierte en la más relevante dentro de la actualización. Su explotación podría tener un impacto significativo en la confidencialidad, integridad y disponibilidad de los sistemas afectados. Las vulnerabilidades restantes cuentan una severidad moderada.

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 tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible.

2. Recursos afectados

- VMware Aria Operations versiones 8.6.x y 8.10.
- VMware Cloud Foundation (VMware Aria Operations) versión 4.x.

3. Análisis técnico

Los detalles de las vulnerabilidades tratadas en este aviso de seguridad son:

CVE-2023-20877: vulnerabilidad de escalada de privilegios, de forma que, un usuario malintencionado autenticado con privilegios de solo lectura puede realizar la ejecución de código que conduce a una escalada de privilegios.

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-2023-20879: vulnerabilidad de escalada de privilegios locales. Un actor malicioso con privilegios administrativos, en la aplicación Aria Operations, puede obtener acceso de root al sistema operativo subyacente.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 6.7

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

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

CVE-2023-20878: vulnerabilidad de deserialización en VMware Aria Operations, de manera que, un actor malicioso con privilegios administrativos puede ejecutar comandos arbitrarios e interrumpir el sistema.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 6.6

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

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

CVE-2023-20880: vulnerabilidad de escalada de privilegios locales, de forma que, un actor malicioso con acceso administrativo al sistema local puede escalar los privilegios a root.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 6.4

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

- **Vector de ataque**: Local
- **Complejidad del ataque**: Alta
- **Privilegios requeridos:** Altos
- **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 corregir las vulnerabilidades descritas desde VMware se recomienda:

- En el caso de la versión 8.10 de VMware Aria Operations, aplicar la actualización 8.10 Hot Fix 4.
- Para la versión 8.6.x de VMware Aria Operations, aplicar la actualización 8.6 Hot Fix 10.
- Port último, para la versión 4.x de VMware Cloud Foundation (VMware Aria Operations) se ofrece una solución alternativa (workaround) disponible desde este enlace.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2023-20877.
- CVE-2023-20878.
- CVE-2023-20879.
- CVE-2023-20880.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA