Basque CyberSecurity Centre

Vulnerabilidades en Aruba Orchestrator

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

Aruba ha lanzado actualizaciones de seguridad para Aruba Orchestrator en donde se abordan correcciones para múltiples vulnerabilidades. Los fallos cuentan con una severidad entre alta y media y son de los siguientes tipos:

- Inyección SQL
- Escalada de privilegios
- Cross-site-scripting
- Bypass de autenticación

Estas vulnerabilidades, de ser explotadas, podrían usarse para:

- Obtener y modificar información sensible
- Permitir a un atacante obtener acceso administrativo en la interfaz de administración web produciendo un compromiso del sistema
- Ejecutar código arbitrario en el navegador de una víctima en el contexto de la interfaz afectada
- Ejecutar comandos arbitrarios como root comprometiendo el sistema al completo
- Permitir que un atacante inicie sesión usando solo un nombre de usuario y contraseña y eludir con éxito los requisitos de MFA (autenticación de múltiples factores)
- Permitir a un atacante autenticado permanecer en el sistema con los permisos de su actual sesión

Los identificadores de todas ellas son: CVE-2022-43519, CVE-2022-43520, CVE-2022-43521, CVE-2022-43522, CVE-2022-43523, CVE-2022-44535, CVE-2022-43524, CVE-2022-44534, CVE-2022-43525, CVE-2022-43526, CVE-2022-43527, CVE-2022-43528, CVE-2022-43529.

2. Recursos afectados

- Aruba EdgeConnect Enterprise Orchestrator (local)
- Aruba EdgeConnect Enterprise Orchestrator como servicio
- Aruba EdgeConnect Enterprise Orchestrator-SP y Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators
- Orchestrator 9.2.1.40179 e inferior
- Orchestrator 9.1.4.40436 e inferior
- Orchestrator 9.0.7.40110 e inferior
- Orchestrator 8.10.23.40015 e inferior
- Cualquier versión anterior de Orchestrator no mencionada específicamente.

3. Análisis técnico

El detalle de las vulnerabilidades tratadas es el siguiente:

Las vulnerabilidades CVE-2022-43519, CVE-2022-43520, CVE-2022-43521, CVE-2022-43522, CVE-2022-43523 son fallos de inyección SQL autenticada en Aruba Administración basada en web de EdgeConnect Enterprise Orchestrator Interfaz.

La métrica de todas ellas es la siguiente:

CVSS Base: 8.8, alta

CWE 89: Neutralización incorrecta de elementos especiales utilizados en un comando SQL (inyección SQL)

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-2022-44535: vulnerabilidad de escalada de privilegios en Aruba EdgeConnect Interfaz de gestión basada en web de Enterprise Orchestrator lo que conduce al compromiso total del sistema

La métrica de la vulnerabilidad es la siguiente:

CVSS Base: 8.8, alta

CWE 284: Control de acceso inadecuado

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-2022-43524: vulnerabilidad en la interfaz de administración basada en web de Aruba EdgeConnect Enterprise Orchestrator podría permitir un atacante

remoto autenticado para realizar un cross-site-scripting (XSS) contra un usuario administrativo de la interfaz. Un exploit exitoso permite a un atacante ejecutar código de script arbitrario en el navegador de una víctima en el contexto de la interfaz afectada.

La métrica de la vulnerabilidad es la siguiente:

CVSS Base: 8.7, alta

CWE 79: Neutralización incorrecta de la entrada durante la generación de la página web (Cross-site Scripting)

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

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

CVE-2022-44534: vulnerabilidad de ejecución de código remoto autenticado en Aruba EdgeConnec Interfaz de gestión basada en web de Enterprise Orchestrator que produce el compromiso total del sistema.

La métrica de la vulnerabilidad es la siguiente:

CVSS Base: 7.2, alta

CWE 94: Control inadecuado de la generación de código (Inyección de código)

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

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

Las vulnerabilidades CVE-2022-43525, CVE-2022-43526, CVE-2022-43527 son fallos de Cross Site Scripting (XSS) en Aruba Interfaz de administración web de EdgeConnect Enterprise Orchestrator.

La métrica de las vulnerabilidades es la siguiente:

CVSS Base: 6.1, media

CWE 94: Control inadecuado de la generación de código (Inyección de código)

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

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

CVE-2022-43528: vulnerabilidad de omisión de autenticación multifactor en Aruba EdgeConnect Enterprise Orchestrator.

La métrica de la vulnerabilidad es la siguiente:

CVSS Base: 4.8, media

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

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

CVE-2022-43529: vulnerabilidad que produce un error al invalidar correctamente la sesión de usuario en Aruba EdgeConnect Enterprise Orchestrator Web-Based Management Interface.

La métrica de la vulnerabilidad es la siguiente:

CVSS Base: 4.6, media

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

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

4. Mitigación / Solución

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

Desde Aruba, según se refleja su nota de seguridad, se recomienda actualizar Aruba EdgeConnect Enterprise Orchestrator a una de las siguientes versiones corregidas para resolver todos los problemas señalados:

Aruba EdgeConnect Enterprise Orchestrator (local)

- Orchestrator 9.2.2.40291 y versiones posteriores
- Orchestrator 9.1.5.40037 y versiones posteriores
- Aruba EdgeConnect Enterprise Orchestrator-as-a-Service
- TAC creará automáticamente un caso de soporte para Aruba (Silver Peak) para Orchestrators alojados que se actualizarán.
- Aruba EdgeConnect Enterprise Orchestrator-SP y ArubaEdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators

También se remarca que los proveedores de servicios deben actualizar a una versión mencionada anteriormente.

5. Referencias Adicionales

- Nota de seguridad de Aruba
- CVE-2022-43519, CVE-2022-43520, CVE-2022-43521, CVE-2022-43522, CVE-2022-43523, CVE-2022-44535, CVE-2022-43524, CVE-2022-44534, CVE-2022-43525, CVE-2022-43526, CVE-2022-43527, CVE-2022-43528, CVE-2022-43529
- Aruba Orchestrator
- CWE 94
- CWE 79
- CWE 284
- CWE 89


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA