Basque CyberSecurity Centre

Vulnerabilidades en productos VMware

BCSC-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Sobre el BCSC 3
1. Aviso de seguridad 4
2. Recursos afectados 5
3. Análisis técnico 6
4. Mitigación / Solución 7
5. Referencias Adicionales 8

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 dos avisos de seguridad, VMSA-2023-0004 y VMSA-2023-0005, donde se tratan una vulnerabilidad de severidad crítica, cuyo identificador es CVE-2023-20858 y una vulnerabilidad de severidad alta, con identificador CVE-2023-20855, respectivamente.

Por una parte, el fallo crítico CVE-2023-20858 podría permitir a un actor malicioso la inyección de código a través de la consola de administración de la herramienta Carbon Black App Control. Por otra, el fallo CVE-2023-20855 puede permitir el acceso a información sensible o conducir a una escalada de privilegios. En ambos casos, la explotación de estas vulnerabilidades tiene un alto impacto en la confidencialidad, integridad y disponibilidad de los sistemas afectados.

2. Recursos afectados

- VMware vRealize Orchestrator version 8.x.
- VMware vRealize Automation version 8.x.
- VMware Cloud Foundation (Cloud Foundation) versión 4.x.
- VMware Carbon Black App Control (App Control) versions 8.7.x, 8.8.x y 8.9.x.

3. Análisis técnico

Los detalles de las vulnerabilidades tratadas en esta actualización son los siguientes:

CVE-2023-20858: vulnerabilidad de inyección de código de manera que un actor malicioso, con acceso privilegiado a la consola de administración de App Control, puede usar una entrada especialmente diseñada que permita el acceso al sistema operativo del servidor subyacente.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 9.1

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

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

CVE-2023-20855: vulnerabilidad de entidad externa XML (XXE) en la que un actor malicioso, con acceso no administrativo a vRealize Orchestrator, puede utilizar entradas especialmente diseñadas para eludir las restricciones de análisis XML que conducen al acceso a información confidencial o una posible 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**

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 remediar el fallo crítico, CVE-2023-20858, VMware recomienda aplicar las actualizaciones de seguridad correspondientes disponibles en su propio aviso:

- Fixed versión para App Control versión 8.9.x disponible en el siguiente enlace.
- Fixed versión para App Control versión 8.8.x disponible en el siguiente enlace.
- Fixed versión para App Control versión 8.7.x disponible en el siguiente enlace.

En cuanto a la vulnerabilidad CVE-2023-20855, VMware, de la misma manera, recomienda aplicar las actualizaciones de seguridad correspondientes disponibles en su propio aviso:

- Fixed Version para VMware vRealize Orchestrator disponible en el siguiente enlace.
- Fixed Version para VMware VMware vRealize Automation disponible en el siguiente enlace.
- Fixed Version para VMware Cloud Foundation (vRealize Automation) disponible en el siguiente enlace.

5. Referencias Adicionales

- VMSA-2023-0004.
- VMSA-2023-0005.
- CVE-2023-20855.
- CVE-2023-20858.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA