Basque CyberSecurity Centre

Vulnerabilidades en productos VMware

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

VMware, empresa proveedora de servicios software de virtualización, ha publicado dos avisos de seguridad, VMSA-2022-0031 y VMSA-2022-033, que contienen dos vulnerabilidades críticas y una alta que afectan a VMware vRealize Network Insight (vRNI), VMware ESXi, VMware Workstation y VMware Fusion.

Primeramente, en lo que respecta al aviso VMSA-2022-0031, se adjunta un error catalogado bajo el identificador CVE-2022-31702 y calificado con una severidad crítica por parte del fabricante, que permite a un atacante remoto ejecutar código arbitrario en el sistema vulnerable. Además, el CVE-2022-31703 cuya puntuación determina que la vulnerabilidad tiene una criticidad alta, puede causar un cruce transversal de directorios en el sistema afectado. Ambos errores se dan en dispositivos VMware vRealize Network Insight (vRNI).

Seguidamente, en lo referente al aviso VMSA-2022-033, cabe destacar que la vulnerabilidad registrada bajo el identificador CVE-2022-31705 y catalogada con una severidad crítica por parte del fabricante, se debe a una escritura fuera de los límites dentro de los sistemas vulnerables.

Cabe destacar que, el CVE-2022-31705 ha sido explotado por parte del investigador Yuhao Jing, siendo premiado a su vez por parte de GeekPwn, un concurso orientado a la explotación de dispositivos y dirigido por una organización cuya sede se encuentra en China.

VMware ya ha publicado el parche oficial mediante los avisos VMSA-2022-0031 y VMSA-2022-033, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir esta y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Análisis técnico

En primera instancia, la vulnerabilidad identificada bajo el CVE-2022-31702 cuya severidad es crítica, contando con una puntuación de 9.8 sobre la escala CVSSv3, permite a un atacante remoto ejecutar comandos shell arbitrarios en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada inadecuada en la *API REST* de vRNI. Un atacante remoto no autenticado puede pasar datos especialmente diseñados al punto final de la *API REST* afectada y ejecutar comandos arbitrarios del sistema operativo en el sistema vulnerable.

Seguidamente, el CVE-2022-31703 que tiene una severidad alta, siendo su puntuación de 7.5 en relación a la escala CVSSv3, aprovecha un error de validación de entrada al procesar secuencias de recorrido de directorios dentro de la *API REST* de vRNI. La explotación exitosa de dicha vulnerabilidad podría permitir a un atacante remoto enviar una solicitud HTTP especialmente diseñada y leer archivos arbitrarios en el sistema.

En cuanto al CVE-2022-31705, cuya severidad es crítica y se le ha asignado una puntuación de 9.3 sobre la escala CVSSv3, existe debido a un *boundary error* dentro del controlador USB 2.0 (EHCI). Un usuario local con privilegios en el sistema operativo invitado puede desencadenar una escritura fuera de los límites y ejecutar código arbitrario como proceso VMX de la máquina virtual que se ejecuta en el host. Cabe destacar que dicho fallo afecta a dispositivos VMware ESXi, VMware Workstation y VMware Fusion.

Finalmente, el investigador anteriormente mencionado Yuhao Jiang, ha publicado mediante su cuenta oficial en Twitter, una prueba de concepto (PoC) en la que muestra los pasos a seguir para explotar la vulnerabilidad asignada al CVE-2022-31705.

Los productos afectados por la anterior vulnerabilidad son los siguientes:

- VMWare vRealize Network Insight versiones 6.7, 6.6, 6.5.X, 6.4, 6.3 y 6.2.
- VMware ESXi versiones 8.0 y 7.0.
- VMware ESXi Cloud Foundation versiones 4.X y 3.X.
- VMware Fusion en sistemas macOS versión 12.X.
- VMware Workstation versiones 16.X.

3. Mitigación / Solución

Como es habitual, para prevenir esta y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

Es importante que se tomen medidas rápidamente para mitigar estos problemas en la implementación. Por ello, dada la gravedad de las vulnerabilidades, se recomienda aplicar las soluciones oficiales propuestas por VMWare, disponibles en los siguientes enlaces:

- Download VMware vRealize Network Insight 6.8.0.
- Addressing CVE-2022-31702 and CVE-2022-31703 in vRNI On-Prem installations (90381).
- VMware ESXi 8.0a Release Notes.
- VMware ESXi 7.0 Update 3i Release Notes.
- Download VMware Fusion 12.2.5.
- Download VMware Workstation Pro 16.2.5.

Asimismo, el fabricante ha proporcionado a los usuarios dos mitigaciones alternativas de seguridad para la vulnerabilidad CVE-2022-31705. En relación a VMware ESXi, se destaca en la publicación correspondiente que los administradores deben asegurarse que el controlador USB no se encuentre activo, debiendo editar la configuración de la máquina virtual, eliminando todos los controladores y aplicando los cambios realizados.

Ilustración 1 Eliminación del controlador USB en el sistema vulnerable

Adicionalmente, en la publicación sobre la mitigación alternativa que afecta a VMware Fusion, se debe seguir los siguientes pasos:

- Seleccionar Ventana > Biblioteca de máquinas virtuales.
- Seleccionar una máquina virtual en la ventana Biblioteca de máquinas virtuales y hacer clic en Configuración.
- En Dispositivos extraíbles en la ventana Configuración, hacer clic en USB y Bluetooth.
- En Opciones USB avanzadas, hacer clic en Quitar controlador USB.
- Hacer clic en Eliminar en el cuadro de diálogo de confirmación.

Finalmente, para VMware Workstation, se detalla que las siguientes instrucciones deben ser aplicadas:

- Seleccionar una máquina virtual en el panel Biblioteca y seleccionar VM > Configuración.
- En el cuadro de diálogo Configuración de la máquina virtual, ir a la pestaña Hardware.
- Seleccionar la entrada Controlador USB y hacer clic en Quitar.

4. Referencias Adicionales

- VMware.
- MITRE: CVE-2022-31702.
- MITRE: CVE-2022-31703.
- MITRE: CVE-2022-31705.
- First organization.
- VMSA-2022-0031.
- VMSA-2022-033.
- VMware vRealize Network Insight (vRNI).
- VMware ESXi.
- VMware Workstation.
- VMware Fusion.
- Twitter: Yuhao Jiang.
- Twitter: PoC de CVE-2022-31705 publicado por Yuhao Jiang.
- Twitter: GeekPwn.
- VRealize Network Insight API.
- CWE-787: Out-of-bounds Write.
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Patch Transversal').
- What is the VMX process and what is it used for
- Boundary error.
- Download VMware vRealize Network Insight 6.8.0.
- Addressing CVE-2022-31702 and CVE-2022-31703 in vRNI On-Prem installations (90381).
- VMware ESXi 8.0a Release Notes.
- VMware ESXi 7.0 Update 3i Release Notes.
- Download VMware Fusion 12.2.5.
- Download VMware Workstation Pro 16.2.5.
- Steps to remove a USB controller from a VMware ESXi virtual machine (87617).
- Remove the USB Controller on VMware Workstation and VMware Fusion (79712).

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA