Actualización de seguridad de Microsoft-Marzo 2024

CYBERZAINTZA-ACTUALIZACIONES-MICROSOFT-2024-MARZO

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

TABLA DE CONTENIDO

1. Resumen ejecutivo 3
2. Recursos afectados 4
3. Análisis técnico 6
4. Mitigación / Solución 17
5. Referencias Adicionales 18

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca 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 la Agencia de Ciberseguridad Vasca 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 la Agencia de Ciberseguridad Vasca. 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.

1. Resumen ejecutivo

Microsoft ha publicado las actualizaciones de seguridad del mes de **marzo de 2024** en las que se corrigen **63 vulnerabilidades**, siendo **2** de ellas calificadas como **críticas**, **57** como **importantes** y **4 sin un valor asignado** que afectan al navegador Edge basado en Chromium y a Microsoft Edge para Android.

Estas vulnerabilidades afectan a productos como Windows Hyper-V, Microsoft Azure Kubernetes Service, Open Management Infrastructure, SQL Server, Visual Studio Code, Microsoft Edge for Android, Microsoft Authenticator y Windows Defender, entre otros.

La clasificación de las vulnerabilidades según su descripción es la siguiente:

- 18 vulnerabilidades de ejecución remota de código.
- 24 vulnerabilidades de elevación de privilegios.
- 6 vulnerabilidades de denegación de servicio.
- 3 vulnerabilidades de spoofing (suplantación).
- 5 vulnerabilidades de divulgación de información.
- 3 vulnerabilidades use after free.
- 4 vulnerabilidades de bypass.

2. Recursos afectados

Las actualizaciones de seguridad del mes de marzo de 2024 están asociadas a vulnerabilidades que afectan a los siguientes productos:

- Windows Defender
- Open Management Infrastructure
- Microsoft Authenticator
- .NET
- Microsoft Azure Kubernetes Service
- Role: Windows Hyper-V
- Skype for Consumer
- Software for Open Networking in the Cloud (SONiC)
- Microsoft Dynamics
- Azure SDK
- Microsoft Office SharePoint
- Windows Kerberos
- Windows USB Hub Driver
- Windows USB Serial Driver
- Windows Hypervisor-Protected Code Integrity
- Windows Update Stack
- Windows Print Spooler Components
- Microsoft Windows SCSI Class System File
- Windows OLE
- Windows Installer
- Microsoft Graphics Component
- Windows AllJoyn API
- Windows Telephony Server
- Windows ODBC Driver
- Microsoft WDAC OLE DB provider for SQL
- Windows USB Print Driver
- Windows Kernel
- Windows NTFS

- Microsoft Teams for Android
- Microsoft WDAC OLE DB provider for SQL
- Microsoft WDAC ODBC Driver
- Windows ODBC Driver
- Windows Cloud Files Mini Filter Driver
- SQL Server
- Visual Studio Code
- Microsoft Edge for Android
- Windows Error Reporting
- Windows Composite Image File System
- Windows Compressed Folder
- Microsoft QUIC
- Windows Standards-Based Storage Management Service
- Microsoft Exchange Server
- Microsoft Office
- Microsoft Intune
- Azure Data Studio
- Outlook for Android

3. Análisis técnico

A continuación, los detalles de las vulnerabilidades de más relevancia corregidas en esta actualización, que son los siguientes:

CVE-2024-21334: vulnerabilidad de ejecución remota de código de Open Management Infrastructure (OMI). Un atacante remoto no autenticado podría acceder a la instancia de OMI desde Internet y enviar solicitudes especialmente diseñadas para desencadenar una vulnerabilidad de use after free.

La métrica de evaluación de la vulnerabilidad se compone de:

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-2024-21400: vulnerabilidad de elevación confidencial de privilegios de contenedor de Microsoft Azure Kubernetes Service. La explotación efectiva de esta vulnerabilidad requiere que un atacante prepare el entorno de destino para mejorar la fiabilidad de la explotación. Un atacante que aprovechara correctamente esta vulnerabilidad podría robar credenciales y afectar a los recursos más allá del ámbito de seguridad administrado por Azure Kubernetes Service Confidential Containers (AKSCC), de forma que, puede acceder al nodo de Kubernetes de AKS que no es de confianza y al contenedor confidencial de AKS para tomar el control de los invitados y contenedores confidenciales más allá de la pila de red a la que podría estar enlazado.

TTP

- Táctica TA0002 – Execution
  - Técnica T1609 – Container Administration Command
- Táctica TA0004 – Privilege Escalation
  - Técnica T1053.007 – Scheduled Task/Job: Container Orchestration Job

Cumplimiento – ENS

SI-7, SI-10, SC-7, CM-5, CM-7, CM-6, AC-2, AC-5, AC-6, AC-3, AC-2, AC-17, IA-8, IA-2

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **9.0**

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

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

CVE-2024-21407: vulnerabilidad de ejecución remota de código de Windows Hyper-V. Este error requeriría que un atacante autenticado en una máquina virtual invitada enviara solicitudes de operación de archivos especialmente diseñadas en la máquina virtual a los recursos de hardware de la máquina virtual, lo que podría dar lugar a la ejecución remota de código en el servidor host. La explotación exitosa de esta vulnerabilidad requiere que un atacante recopile información específica del entorno y realice acciones adicionales antes de la explotación para preparar el entorno de destino.
TTP

- Táctica TA0043 – Reconnaissance
  - Técnica T1595 – Escaneo activo
  - Técnica T1592 – Gather Victim Host Information
- Táctica TA0005 – Defense Evasion
- Táctica TA0007 – Discovery
  - Técnica T1497 – Virtualization/Sandbox Evasion

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.1**

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

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

CVE-2024-21408: vulnerabilidad de denegación de servicio en Windows Hyper-V.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **5.5**

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

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

A continuación, se detalla la lista con todas las vulnerabilidades identificadas:

➢ Las vulnerabilidades identificadas por los CVE marcados en color rojo representan a aquellas que se conoce que están siendo explotadas, o que tienen el potencial de serlo, en función del estado de la amenaza. Este riesgo de explotación se encuentra presente en la última versión del software suministrado por el fabricante.

CVE	Descripción	Severidad	Divulgado	Explotado	CVSS	Soluciones alternativas
CVE-2024-21407	Vulnerabilidad de ejecución remota de código de Windows Hyper-V	**Crítica**	No	No	8.1	No
CVE-2024-21408	Vulnerabilidad de denegación de servicio de Windows Hyper-V	**Crítica**	No	No	5.5	No
CVE-2024-21334	Vulnerabilidad de ejecución remota de código de Open Management Infrastructure (OMI)	Importante	No	No	9.8	Sí
CVE-2024-21400	Vulnerabilidad de elevación confidencial de	Importante	No	No	9.0	No

	privilegios de contenedor de Microsoft Azure Kubernetes Service					
CVE-2024-21411	Vulnerabilidad de ejecución remota de código de Skype for Consumer	Importante	No	No	8.8	No
CVE-2024-21441	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21444	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21450	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21451	Vulnerabilidad de ejecución remota de código del controlador ODBC de Microsoft	Importante	No	No	8.8	No
CVE-2024-26159	Vulnerabilidad de ejecución remota de código del controlador	Importante	No	No	8.8	No

	ODBC de Microsoft					
CVE-2024-26198	Vulnerabilidad de ejecución remota de código de Microsoft Exchange Server	Importante	No	No	8.8	No
CVE-2024-26161	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-26164	Vulnerabilidad de ejecución remota de código de Microsoft Django Backend para SQL Server	Importante	No	No	8.8	No
CVE-2024-21435	Vulnerabilidad de ejecución remota de código OLE de Windows	Importante	No	No	8.8	No
CVE-2024-21440	Vulnerabilidad de ejecución remota de código del controlador ODBC de Microsoft	Importante	No	No	8.8	No
CVE-2024-26162	Vulnerabilidad de ejecución remota de código del controlador ODBC de Microsoft	Importante	No	No	8.8	No
CVE-2024-26166	Vulnerabilidad de ejecución remota de código del	Importante	No	No	8.8	No

	proveedor OLE DB de Microsoft WDAC para SQL Server					
CVE-2024-26165	Vulnerabilidad de elevación de privilegios de Visual Studio Code	Importante	No	No	8.8	No
CVE-2024-21418	Software para redes abiertas en la nube (SONiC) Vulnerabilidad de elevación de privilegios	Importante	No	No	7.8	No
CVE-2024-21426	Vulnerabilidad de ejecución remota de código de Microsoft SharePoint Server	Importante	No	No	7.8	No
CVE-2024-21442	Vulnerabilidad de elevación de privilegios del controlador de impresión USB de Windows	Importante	No	No	7.8	No
CVE-2024-21446	Vulnerabilidad de elevación de privilegios NTFS	Importante	No	No	7.8	No
CVE-2024-26199	Vulnerabilidad de elevación de privilegios de Microsoft Office	Importante	No	No	7.8	No
CVE-2024-21330	Vulnerabilidad de elevación de privilegios de Open Management Infrastructure (OMI)	Importante	No	No	7.8	No
CVE-2024-21431	Vulnerabilidad de omisión de la función de	Importante	No	No	7.8	No

	seguridad de integridad de código protegida por hipervisor (HVCI)					
CVE-2024-21434	Vulnerabilidad de elevación de privilegios de archivos del sistema de clase SCSI de Microsoft Windows	Importante	No	No	7.8	No
CVE-2024-21436	Vulnerabilidad de elevación de privilegios de Windows Installer	Importante	No	No	7.8	No
CVE-2024-21437	Vulnerabilidad de elevación de privilegios del componente de gráficos de Windows	Importante	No	No	7.8	No
CVE-2024-26169	Vulnerabilidad de elevación de privilegios del servicio de informes de errores de Windows	Importante	No	No	7.8	No
CVE-2024-26170	Vulnerabilidad de elevación de privilegios del sistema de archivos de imagen compuesta de Windows (CimFS)	Importante	No	No	7.8	No
CVE-2024-26173	Vulnerabilidad de elevación de privilegios del kernel de Windows	Importante	No	No	7.8	No

CVE-2024-26176	Vulnerabilidad de elevación de privilegios del kernel de Windows	Importante	No	No	7.8	No
CVE-2024-26178	Vulnerabilidad de elevación de privilegios del kernel de Windows	Importante	No	No	7.8	No
CVE-2024-26182	Vulnerabilidad de elevación de privilegios del kernel de Windows	Importante	No	No	7.8	No
CVE-2024-21419	Vulnerabilidad de scripting entre sitios de Microsoft Dynamics 365 (on-premises)	Importante	No	No	7.6	No
CVE-2024-21392	Vulnerabilidad de denegación de servicio de .NET y Visual Studio	Importante	No	No	7.5	No
CVE-2024-21421	Vulnerabilidad de suplantación de identidad del SDK de Azure	Importante	No	No	7.5	No
CVE-2024-21438	Vulnerabilidad de denegación de servicio de la API de Microsoft AllJoyn	Importante	No	No	7.5	No
CVE-2024-26190	Vulnerabilidad de denegación de servicio de Microsoft QUIC	Importante	No	No	7.5	No
CVE-2024-21427	Vulnerabilidad de omisión de características de seguridad de Windows Kerberos	Importante	No	No	7.5	No

CVE-2024-26204	Vulnerabilidad de divulgación de información de Outlook para Android	Importante	No	No	7.5	No
CVE-2024-21443	Vulnerabilidad de elevación de privilegios del kernel de Windows	Importante	No	No	7.3	No
CVE-2024-26203	Vulnerabilidad de elevación de privilegios de Azure Data Studio	Importante	No	No	7.3	No
CVE-2024-21390	Vulnerabilidad de elevación de privilegios de Microsoft Authenticator	Importante	No	No	7.1	No
CVE-2024-21439	Vulnerabilidad de elevación de privilegios del servidor de telefonía de Windows	Importante	No	No	7.0	No
CVE-2024-21445	Vulnerabilidad de elevación de privilegios del controlador de impresión USB de Windows	Importante	No	No	7.0	No
CVE-2024-21432	Vulnerabilidad de elevación de privilegios de la pila de Windows Update	Importante	No	No	7.0	No
CVE-2024-21433	Vulnerabilidad de elevación de privilegios de Windows Print Spooler	Importante	No	No	7.0	No
CVE-2024-21429	Vulnerabilidad de ejecución remota de código del	Importante	No	No	6.8	No

	controlador del concentrador USB de Windows					
CVE-2024-26201	Vulnerabilidad de elevación de privilegios del agente Linux de Microsoft Intune	Importante	No	No	6.6	No
CVE-2024-26197	Vulnerabilidad de denegación de servicio del servicio de administración de almacenamiento basado en estándares de Windows	Importante	No	No	6.5	No
CVE-2024-26185	Vulnerabilidad de manipulación de carpetas comprimidas de Windows	Importante	No	No	6.5	No
CVE-2023-28746	Intel: Muestreo de datos de archivos de registro (RFDS)	Importante	No	No	6.5	No
CVE-2024-21430	Vulnerabilidad de ejecución remota de código del protocolo SCSI (UAS) conectado a USB de Windows	Importante	No	No	5.7	No
CVE-2024-20671	Vulnerabilidad de omisión de características de seguridad de Microsoft Defender	Importante	No	No	5.5	No
CVE-2024-26160	Vulnerabilidad de divulgación de información	Importante	No	No	5.5	No

	del controlador de mini filtro de archivos en la nube de Windows					
CVE-2024-26174	Vulnerabilidad de divulgación de información del kernel de Windows	Importante	No	No	5.5	No
CVE-2024-26177	Vulnerabilidad de divulgación de información del kernel de Windows	Importante	No	No	5.5	No
CVE-2024-26181	Vulnerabilidad de denegación de servicio del kernel de Windows	Importante	No	No	5.5	No
CVE-2024-21448	Vulnerabilidad de divulgación de información de Microsoft Teams para Android	Importante	No	No	5.0	No
CVE-2024-26167	Vulnerabilidad de suplantación de identidad de Microsoft Edge para Android	Sin valor asignado	No	No	4.3	No
CVE-2024-2173	Chromium: Acceso a memoria fuera de límites en V8	Sin valor asignado	No	No	4.3	No
CVE-2024-2174	Chromium: Implementación inapropiada en V8	Sin valor asignado	No	No	4.3	No
CVE-2024-2176	Chromium: Use after free en FedCM	Sin valor asignado	No	No	4.3	No

4. Mitigación / Solución

Para la mitigación y la corrección de todas las vulnerabilidades, Microsoft publica las actualizaciones de seguridad pertinentes junto con sus release notes, las cuales están disponibles en Security Update Guide.

5. Referencias Adicionales

- March 2024 Security Updates.
- Security Update Guide - Microsoft.
- Zero Day initiative-The March 2024 Security Update Review.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY