Actualización de seguridad de Microsoft-Febrero 2024

CYBERZAINTZA-ACTUALIZACIONES-MICROSOFT-2024-FEBRERO

TLP: CLEAR

www.ciberseguridad.eus

TABLA DE CONTENIDO

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 **febrero de 2024** en las que se corrigen **80 vulnerabilidades**, siendo **5** de ellas calificadas como **críticas**, **66** como **importantes, 3 moderadas** y **6 sin un valor asignado** que afectan al navegador Edge basado en Chromium y a CBL-Mariner, la distribución Linux desarrollada por Microsoft.

Dentro de ellas hay **5 vulnerabilidades 0-day**, CVE-2024-21351, CVE-2024-21626, CVE-2024-1060, CVE-2024-1059, CVE-2024-1077, **todas ellas siendo explotadas**.

Estas vulnerabilidades afectan a productos como Azure DevOps, Microsoft Office, Azure Stack, Windows Hyper-V, Skype for Business, Microsoft Teams for Android, Microsoft Defender for Endpoint, Microsoft Dynamics, Azure Connected Machine Agent, Windows Kernel, Windows USB Serial Driver, entre otros.

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

- 31 vulnerabilidades de ejecución remota de código.
- 16 vulnerabilidades de elevación de privilegios.
- 8 vulnerabilidades de denegación de servicio.
- 6 vulnerabilidades de spoofing (suplantación).
- 5 vulnerabilidades de divulgación de información.
- 4 vulnerabilidades Use After Free.
- 4 vulnerabilidades de Cross-site Scripting.
- 3 vulnerabilidades de bypass.
- 1 vulnerabilidad de desbordamiento del búfer del Heap.
- 1 vulnerabilidad en CLB-Mariner.
- 1 vulnerabilidad de complejidad en la verificación para agotar los recursos del CPU.

2. Recursos afectados

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

- Azure DevOps
- Microsoft Office
- Azure Stack
- Windows Hyper-V
- Skype for Business
- Trusted Compute Base
- Microsoft Defender for Endpoint
- Microsoft Dynamics
- Azure Connected Machine Agent
- Windows Kernel
- Windows USB Serial Driver
- Role: DNS Server
- Windows Internet Connection Sharing (ICS)
- Windows Win32K - ICOMP
- SQL Server
- Microsoft ActiveX
- Microsoft WDAC OLE DB provider for SQL
- Windows SmartScreen
- Microsoft WDAC ODBC Driver
- Windows Message Queuing
- Windows LDAP - Lightweight Directory Access Protocol
- Windows Internet Connection Sharing (ICS)
- Azure Site Recovery
- Windows OLE
- Microsoft Teams for Android
- Microsoft Azure Kubernetes Service
- Microsoft Windows DNS
- Microsoft Office Outlook

- Microsoft Office Word
- Azure Active Directory
- Microsoft Office OneNote
- .NET
- Azure File Sync
- Microsoft Edge (Chromium-based)
- Microsoft Azure Kubernetes Service
- Microsoft Windows
- Microsoft Exchange Server
- Internet Shortcut Files

3. Análisis técnico

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

- Los detalles de las **vulnerabilidades 0-day** tratadas en esta actualización son:

CVE-2024-1060: vulnerabilidad Use after free en Canvas.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.8**

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

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

CVE-2024-1059: vulnerabilidad Use after free en WebRTC.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.8**

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

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

CVE-2024-1077: vulnerabilidad Use after free en Network.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.8**

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

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**

- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Requerida
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-21626: Runc es una herramienta CLI para generar y ejecutar contenedores en Linux de acuerdo con la especificación OCI. En runc 1.1.11 y versiones anteriores, debido a una fuga interna del descriptor de archivos, un atacante podía hacer que un proceso de contenedor recién generado tuviera un directorio de trabajo en el espacio de nombres del sistema de archivos host, lo que permitía un escape del contenedor al dar acceso al sistema de archivos host. El mismo ataque podría ser utilizado por una imagen maliciosa para permitir que un proceso contenedor obtenga acceso al sistema de archivos host. Las variantes de los ataques 1 y 2 también podrían usarse para sobrescribir binarios de host semiarbitrarios, lo que permite escapes completos de contenedores. Runc 1.1.12 incluye parches para este problema.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.6**

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

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

CVE-2024-21351: Vulnerabilidad de bypass en características de seguridad SmartScreen de Windows. La vulnerabilidad permite a un actor malintencionado inyectar código en SmartScreen y potencialmente obtener la ejecución de código, lo que podría conducir a cierta exposición de datos, falta de disponibilidad del sistema o ambos. Para su explotación, el atacante debe enviar al usuario un archivo malintencionado y convencerlo de que lo abra.

TTP

- Táctica TA0002 – Execution
- Técnica T1204 – User Execution

Cumplimiento – ENS

MP.S.1, OP.EXP.5, OP.EXP.4, OP.MON.1, OP.EXP.6, OP.EXP.2, OP.ACC.2, MP.COM.1, MP.COM.2

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.6**

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

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

➢ Los detalles de las **vulnerabilidades de severidad crítica** son:

CVE-2024-21413: vulnerabilidad de ejecución remota de código de Microsoft Outlook. La explotación exitosa de esta vulnerabilidad permitiría a un atacante omitir la vista protegida de Office y abrirla en modo de edición en lugar de en modo protegido.

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-2024-21410: vulnerabilidad de elevación de privilegios de Microsoft Exchange Server. Un atacante podría dirigirse a un cliente NTLM como Outlook con una vulnerabilidad de tipo de fuga de credenciales NTLM. A continuación, las credenciales filtradas se pueden retransmitir en el servidor de Exchange para obtener privilegios como cliente de la víctima y realizar operaciones en el servidor de Exchange en nombre de la víctima. Para obtener más información acerca de la compatibilidad de Exchange Server con la protección ampliada

para la autenticación (EPA), consulte Configurar la protección ampliada de Windows en Exchange Server. Un atacante que aprovechara con éxito esta vulnerabilidad podría retransmitir el hash Net-NTLMv2 filtrado de un usuario contra un Exchange Server vulnerable y autenticarse como el usuario.

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-2024-21380: vulnerabilidad de divulgación de información de Microsoft Dynamics Business Central/NAV. La explotación exitosa de esta vulnerabilidad requiere que un atacante gane una condición de carrera. El usuario tendría que hacer clic en una URL especialmente diseñada para ser comprometida por el atacante.

TTP

- Táctica TA0001 – Initial Access
- Técnica T1566 – Phishing
- Táctica TA0002 – Execution
- Técnica T1204 – User Execution

Cumplimiento – ENS

MP.S.1, OP.EXP.5, OP.EXP.4, OP.MON.1, OP.EXP.6, OP.EXP.2, OP.ACC.2, MP.COM.1, MP.COM.2, OP.ACC.1, OP.ACC.5, OP.EXP.2

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.0**

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

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

- **Disponibilidad: Alta**

CVE-2024-21357: vulnerabilidad de ejecución remota de código de multidifusión general pragmática (PGM) de Windows. La explotación exitosa de esta vulnerabilidad requiere que un atacante realice acciones adicionales antes de la explotación para preparar el entorno de destino. Este ataque se limita a los sistemas conectados al mismo segmento de red que el atacante. El ataque no se puede realizar en varias redes (por ejemplo, una WAN) y se limitaría a los sistemas del mismo conmutador de red o red virtual.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.5**

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

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

CVE-2024-20684: vulnerabilidad de denegación de servicio de Windows Hyper-V. La explotación correcta de esta vulnerabilidad podría permitir que un invitado de Hyper-V afecte a la funcionalidad del host de Hyper-V.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **6.5**

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

- **Vector de ataque**: **Local**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con 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-2024-21413	Vulnerabilidad de ejecución remota de código de Microsoft Outlook	**Crítica**	No	No	9.8	No
CVE-2024-21410	Vulnerabilidad de elevación de privilegios de Microsoft Exchange Server	**Crítica**	No	No	9.8	Sí
CVE-2024-21380	Vulnerabilidad de divulgación de información de Microsoft Dynamics Business Central/NAV	**Crítica**	No	No	8.0	No
CVE-2024-21357	Vulnerabilidad de ejecución remota de código de multidifusión general pragmática (PGM) de Windows	**Crítica**	No	No	7.5	No
CVE-2024-20684	Vulnerabilidad de denegación de servicio de Windows Hyper-V	**Crítica**	No	No	6.5	No
CVE-2024-21401	Vulnerabilidad de elevación de privilegios del complemento de inicio de sesión único	Importante	No	No	9.8	No

	de Microsoft Entra Jira					
CVE-2024-21376	Vulnerabilidad de ejecución remota de código de contenedor confidencial de Microsoft Azure Kubernetes Service	Importante	No	No	9.0	No
CVE-2024-21403	Vulnerabilidad de elevación confidencial de privilegios de contenedor de Microsoft Azure Kubernetes Service	Importante	No	No	9.0	No
CVE-2024-21349	Vulnerabilidad de ejecución remota de código de objetos de datos ActiveX de Microsoft	Importante	No	No	8.8	No
CVE-2024-21350	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21352	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No

CVE-2024-21358	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21360	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21361	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21366	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21369	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No

CVE-2024-21372	Vulnerabilidad de ejecución remota de código OLE de Windows	Importante	No	No	8.8	No
CVE-2024-21375	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21420	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21345	Vulnerabilidad de elevación de privilegios del kernel de Windows	Importante	No	No	8.8	No
CVE-2024-21353	Vulnerabilidad de ejecución remota de código del controlador ODBC de Microsoft WDAC	Importante	No	No	8.8	No
CVE-2024-21359	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No

CVE-2024-21365	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21367	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21368	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21370	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2024-21391	Vulnerabilidad de ejecución remota de código del proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No

CVE-2024-21395	Vulnerabilidad de scripting entre sitios de Microsoft Dynamics 365 (on-premises)	Importante	No	No	8.2	No
CVE-2024-21412	Vulnerabilidad de omisión de la función de seguridad de archivos de acceso directo de Internet	Importante	No	Sí	8.1	No
CVE-2024-21378	Vulnerabilidad de ejecución remota de código de Microsoft Outlook	Importante	No	No	8.0	No
CVE-2024-21338	Vulnerabilidad de elevación de privilegios del kernel de Windows	Importante	No	No	7.8	No
CVE-2024-21354	Vulnerabilidad de elevación de privilegios de Microsoft Message Queue Server (MSMQ)	Importante	No	No	7.8	No
CVE-2024-21379	Vulnerabilidad de ejecución remota de código de Microsoft Word	Importante	No	No	7.8	No
CVE-2024-20673	Vulnerabilidad de ejecución remota de código de Microsoft Office	Importante	No	No	7.8	No
CVE-2024-21315	Vulnerabilidad de elevación de privilegios	Importante	No	No	7.8	No

	de Microsoft Defender para Endpoint Protection					
CVE-2024-21346	Vulnerabilidad de elevación de privilegios de Win32k	Importante	No	No	7.8	No
CVE-2024-21363	Vulnerabilidad de ejecución remota de código de Microsoft Message Queue Server (MSMQ)	Importante	No	No	7.8	No
CVE-2024-21384	Vulnerabilidad de ejecución remota de código de Microsoft Office OneNote	Importante	No	No	7.8	No
CVE-2024-21327	Vulnerabilidad de scripting entre sitios de Microsoft Dynamics 365 Customer Engagement	Importante	No	No	7.6	No
CVE-2024-21389	Vulnerabilidad de scripting entre sitios de Microsoft Dynamics 365 (on-premises)	Importante	No	No	7.6	No
CVE-2024-21393	Vulnerabilidad de scripting entre sitios de Microsoft Dynamics 365 (on-premises)	Importante	No	No	7.6	No
CVE-2024-21394	Vulnerabilidad de suplantación de identidad de	Importante	No	No	7.6	No

	Dynamics 365 Field Service					
CVE-2024-21396	Vulnerabilidad de suplantación de identidad de Dynamics 365 Sales	Importante	No	No	7.6	No
CVE-2024-21328	Vulnerabilidad de suplantación de identidad de Dynamics 365 Sales	Importante	No	No	7.6	No
CVE-2024-20667	Vulnerabilidad de ejecución remota de código de Azure DevOps Server	Importante	No	No	7.5	No
CVE-2023-50387	MITRE: la complejidad de la verificación de DNSSEC se puede explotar para agotar los recursos de la CPU y detener los solucionadores de DNS	Importante	No	No	7.5	No
CVE-2024-21386	Vulnerabilidad de denegación de servicio de .NET	Importante	No	No	7.5	No
CVE-2024-21404	Vulnerabilidad de denegación de servicio de .NET	Importante	No	No	7.5	Sí
CVE-2024-21342	Vulnerabilidad de denegación de servicio del cliente DNS de Windows	Importante	No	No	7.5	No

CVE-2024-21347	Vulnerabilidad de ejecución remota de código del controlador ODBC de Microsoft	Importante	No	No	7.5	No
CVE-2024-21348	Vulnerabilidad de denegación de servicio de conexión compartida a Internet (ICS)	Importante	No	No	7.5	No
CVE-2024-21406	Vulnerabilidad de suplantación de identidad del servicio de impresión de Windows	Importante	No	No	7.5	No
CVE-2024-21329	Vulnerabilidad de elevación de privilegios de Azure Connected Machine Agent	Importante	No	No	7.3	No
CVE-2024-21402	Vulnerabilidad de elevación de privilegios de Microsoft Outlook	Importante	No	No	7.1	No
CVE-2024-21377	Vulnerabilidad de divulgación de información DNS de Windows	Importante	No	No	7.1	No
CVE-2024-21371	Vulnerabilidad de elevación de privilegios del kernel de Windows	Importante	No	No	7.0	No
CVE-2024-21355	Vulnerabilidad de elevación de privilegios de Microsoft Message	Importante	No	No	7.0	No

	Queue Server (MSMQ)					
CVE-2024-21405	Vulnerabilidad de elevación de privilegios de Microsoft Message Queue Server (MSMQ)	Importante	No	No	7.0	No
CVE-2024-21381	Vulnerabilidad de suplantación de identidad de Microsoft Azure Active Directory B2C	Importante	No	No	6.8	No
CVE-2024-21341	Vulnerabilidad de ejecución remota de código del kernel de Windows	Importante	No	No	6.8	No
CVE-2024-20679	Vulnerabilidad de suplantación de identidad de Azure Stack Hub	Importante	No	No	6.5	No
CVE-2024-21356	Vulnerabilidad de denegación de servicio del protocolo ligero de acceso a directorios (LDAP) de Windows	Importante	No	No	6.5	No
CVE-2024-21339	Vulnerabilidad de ejecución remota de código del controlador principal genérico USB de Windows	Importante	No	No	6.4	No

CVE-2024-21343	Vulnerabilidad de denegación de servicio de traducción de direcciones de red (NAT) de Windows	Importante	No	No	5.9	No
CVE-2024-21344	Vulnerabilidad de denegación de servicio de traducción de direcciones de red (NAT) de Windows	Importante	No	No	5.9	No
CVE-2024-20695	Vulnerabilidad de divulgación de información de Skype Empresarial	Importante	No	No	5.7	No
CVE-2024-21362	Vulnerabilidad de omisión de características de seguridad del kernel de Windows	Importante	No	No	5.5	No
CVE-2024-21397	Vulnerabilidad de elevación de privilegios de Microsoft Azure File Sync	Importante	No	No	5.3	No
CVE-2024-21374	Divulgación de información de Microsoft Teams para Android	Importante	No	No	5.0	No
CVE-2024-21340	Vulnerabilidad de divulgación de información del kernel de Windows	Importante	No	No	4.6	No
CVE-2024-21304	Vulnerabilidad de elevación de privilegios de la base de cómputo de confianza	Importante	No	No	4.1	No

CVE-2024-21364	Vulnerabilidad de elevación de privilegios de Microsoft Azure Site Recovery	Moderada	No	No	9.3	No
CVE-2024-21399	Vulnerabilidad de ejecución remota de código de Microsoft Edge (basado en Chromium)	Moderada	No	No	8.3	No
CVE-2024-21351	Vulnerabilidad de omisión de la característica de seguridad SmartScreen de Windows	Moderada	No	Sí	7.6	No
CVE-2024-21626	Mariner	Sin valor asignado	No	Sí	8.6	No
CVE-2024-1060	Chromium: Use after free en Canvas	Sin valor asignado	No	Sí	8.1	No
CVE-2024-1059	Chromium: Use after free en WebRTC	Sin valor asignado	No	Sí	8.1	No
CVE-2024-1077	Chromium: Use after free en Network	Sin valor asignado	No	Sí	8.1	No
CVE-2024-1283	Chromium: Heap buffer overflow en Skia	Sin valor asignado				No
CVE-2024-1284	Chromium: Use after free en Mojo	Sin valor asignado				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

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


cyber
zaintza
BASQUE CYBERSECURITY AGENCY