Basque CyberSecurity Centre

Actualización de seguridad de Microsoft-Marzo 2023

BCSC-ACTUALIZACIONES-MICROSOFT-2023-MARZO

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. Resumen ejecutivo

Microsoft ha publicado las actualizaciones de seguridad del mes de marzo de 2023 en las que se corrigen 104 vulnerabilidades, siendo 9 de ellas calificadas como críticas, 70 como importantes, 1 moderada y 24 sin un valor asignado que incluyen, por una parte, al navegador Edge basado en Chromium y a la distribución de Linux CBL-Mariner por otra.

Dentro de ellas hay **2 vulnerabilidades zero-day,** una que ha sido **divulgada públicamente y está siendo explotada,** con identificador CVE-2023-24880 y otra **siendo explotada,** con identificador CVE-2023-23397.

Estas vulnerabilidades afectan a productos como Microsoft Office Outlook, Office para Android, Internet Control Message Protocol, Microsoft Edge basado en Chromium, Windows Hyper-V, Windows Cryptographic Services y Windows Defender entre otros.

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

- 27 vulnerabilidades de ejecución remota de código.
- 21 vulnerabilidades de elevación de privilegios.
- 15 vulnerabilidades de divulgación de información.
- 2 vulnerabilidad de bypass.
- 4 vulnerabilidades de denegación de servicio.
- 6 vulnerabilidades de spoofing.
- 5 vulnerabilidades de Cross-site Scripting (XSS).
- 3 vulnerabilidad de Use-After-Free.
- 1 vulnerabilidad de Desbordamiento del búfer de pila.
- 3 vulnerabilidad de confusión de tipos.
- 3 vulnerabilidades de desbordamiento del búfer del heap.
- 6 vulnerabilidades de aplicación insuficiente de las políticas.
- 5 vulnerabilidades de implementación inadecuada.
- 3 vulnerabilidades que afectan a CBL-Mariner.

2. Recursos afectados

Las actualizaciones de seguridad del mes de marzo de 2023 están asociadas a vulnerabilidades que afectan a los siguientes productos:

- Azure
- Client Server Run-time Subsystem (CSRSS)
- Internet Control Message Protocol (ICMP)
- Microsoft Bluetooth Driver
- Microsoft Dynamics
- Microsoft Edge (Chromium-based)
- Microsoft Graphics Component
- Microsoft Office Excel
- Microsoft Office Outlook
- Microsoft Office SharePoint
- Microsoft OneDrive
- Microsoft PostScript Printer Driver
- Microsoft Printer Drivers
- Microsoft Windows Codecs Library
- Office for Android
- Remote Access Service Point-to-Point Tunneling Protocol
- Role: DNS Server
- Role: Windows Hyper-V
- Service Fabric
- Visual Studio
- Windows Accounts Control
- Windows Bluetooth Service
- Windows Central Resource Manager
- Windows Cryptographic Services
- Windows Defender
- Windows HTTP Protocol Stack
- Windows HTTP.sys
- Windows Internet Key Exchange (IKE) Protocol

- Windows Kernel
- Windows Partition Management Driver
- Windows Point-to-Point Protocol over Ethernet (PPPoE)
- Windows Remote Procedure Call
- Windows Remote Procedure Call Runtime
- Windows Resilient File System (ReFS)
- Windows Secure Channel
- Windows SmartScreen
- Windows TPM
- Windows Win32K

3. Análisis técnico

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

Las 2 vulnerabilidades zero-day reportadas son:

CVE-2023-23397: vulnerabilidad de elevación de privilegios en Microsoft Outlook de manera que un atacante que aprovechara esta vulnerabilidad podría tener acceso al hash Net-NTLMv2 de un usuario, que podría usarse como base de un ataque de retransmisión NTLM contra otro servicio para autenticarse como 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-2023-24880: vulnerabilidad de omisión de la característica de seguridad en SmartScreen de Windows de forma que un atacante puede crear un archivo malintencionado que evadiría las defensas de la marca de la Web (MOTW), lo que provocaría una pérdida limitada de integridad y disponibilidad de características de seguridad como Vista protegida en Microsoft Office, que dependen del etiquetado MOTW.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 5.4

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

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

Las vulnerabilidades críticas corregidas son:

CVE-2023-23392: vulnerabilidad de ejecución remota de código en la pila de protocolo HTTP debido a que en la mayoría de las situaciones, un atacante no autenticado podría enviar un paquete especialmente diseñado a un servidor de destino utilizando la pila de protocolos HTTP (http.sys) para procesar paquetes.

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-2023-21708: vulnerabilidad de ejecución remota de código en tiempo de ejecución en llamada a procedimiento remoto de forma que para aprovechar esta vulnerabilidad, un atacante no autenticado tendría que enviar una llamada RPC especialmente diseñada a un host RPC. Esto podría provocar la ejecución remota de código en el servidor con los mismos permisos que el servicio RPC.

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-2023-23415: vulnerabilidad de ejecución remota de código en el Protocolo de mensajes de control de Internet (ICMP). Un atacante podría enviar un error de protocolo de bajo nivel que contenga un paquete IP fragmentado dentro de otro paquete ICMP en su encabezado a la máquina de destino. Para desencadenar la ruta de código vulnerable, una aplicación en el destino debe estar enlazada a un socket sin formato.

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-2023-1017: vulnerabilidad de elevación de privilegios en la biblioteca de módulos TPM2.0. Al aprovechar los comandos malintencionados de TPM de una máquina virtual invitada a un destino que ejecuta Hyper-V, un atacante puede provocar una escritura fuera de los límites en la partición raíz.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.8

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

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

CVE-2023-1018: vulnerabilidad de elevación de privilegios en la biblioteca de módulos TPM2.0.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.8

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

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

- **Disponibilidad:** Ninguna

CVE-2023-23416: vulnerabilidad de ejecución remota de código en Servicios criptográficos de Windows. Para una explotación exitosa, es necesario importar un certificado malicioso en un sistema afectado. Un atacante podría cargar un certificado en un servicio que procesa o importa certificados, o un atacante podría convencer a un usuario autenticado para que importe un certificado en su sistema.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.4

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

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

CVE-2023-23404: vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a punto en Windows. Un atacante no autenticado podría enviar una solicitud de conexión especialmente diseñada a un servidor RAS, lo que podría provocar la ejecución remota de código (RCE) en el equipo servidor RAS.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.1

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

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

CVE-2023-23411: vulnerabilidad de denegación de servicio en Windows Hyper-V. Una explotación correcta de esta vulnerabilidad podría permitir que un invitado de Hyper-V afectara 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:

CVE	Descripción	Severidad	Divulgado	Explotado	CVSS
CVE-2023-23392	Vulnerabilidad de ejecución remota de código en la pila de protocolo HTTP	**Crítica**	No	No	9.8
CVE-2023-23397	Vulnerabilidad de elevación de privilegios en Microsoft Outlook	**Crítica**	No	Sí	9.8
CVE-2023-21708	Vulnerabilidad de ejecución remota de código en tiempo de ejecución remota de llamada a procedimiento remoto	**Crítica**	No	No	9.8
CVE-2023-23415	Vulnerabilidad de ejecución remota de código en el Protocolo de mensajes de control de Internet (ICMP)	**Crítica**	No	No	9.8
CVE-2023-1017	CERT/CC: Vulnerabilidad de elevación de privilegios en la biblioteca de módulos TPM2.0	**Crítica**	No	No	8.8
CVE-2023-1018	CERT/CC: Vulnerabilidad de elevación de privilegios en la biblioteca de módulos TPM2.0	**Crítica**	No	No	8.8

CVE-2023-23416	Vulnerabilidad de ejecución remota de código en Servicios criptográficos de Windows	**Crítica**	No	No	8.4
CVE-2023-23404	Vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a punto en Windows	**Crítica**	No	No	8.1
CVE-2023-23411	Vulnerabilidad de denegación de servicio en Windows Hyper-V	**Crítica**	No	No	6.5
CVE-2023-22490	GitHub: Vulnerabilidad de divulgación de información en mingit	Importante	No	No	9.8
CVE-2023-23388	Vulnerabilidad de elevación de privilegios en el controlador Bluetooth de Windows	Importante	No	No	8.8
CVE-2023-23403	Vulnerabilidad de ejecución remota de código en el controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	8.8
CVE-2023-23406	Vulnerabilidad de ejecución remota de código en el controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	8.8
CVE-2023-23413	Vulnerabilidad de ejecución remota de código en el controlador de impresora de clase	Importante	No	No	8.8

	PostScript y PCL6 de Microsoft				
CVE-2023-24864	Vulnerabilidad de elevación de privilegios en el controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	8.8
CVE-2023-24867	Vulnerabilidad de ejecución remota de código en el controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	8.8
CVE-2023-24907	Vulnerabilidad de ejecución remota de código en el controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	8.8
CVE-2023-24868	Vulnerabilidad de ejecución remota de código en el controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	8.8
CVE-2023-24909	Vulnerabilidad de ejecución remota de código en el controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	8.8
CVE-2023-24871	Vulnerabilidad de ejecución remota de código en el servicio Bluetooth de Windows	Importante	No	No	8.8
CVE-2023-24872	Vulnerabilidad de ejecución remota de código en el controlador de impresora de clase	Importante	No	No	8.8

	PostScript y PCL6 de Microsoft				
CVE-2023-24913	Vulnerabilidad de ejecución remota de código en el controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	8.8
CVE-2023-24876	Vulnerabilidad de ejecución remota de código en el controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	8.8
CVE-2023-23383	Vulnerabilidad de suplantación de identidad en el Explorador de Service Fabric	Importante	No	No	8.2
CVE-2023-23405	Vulnerabilidad de ejecución remota de código en tiempo de ejecución remota de llamada a procedimiento remoto	Importante	No	No	8.1
CVE-2023-24908	Vulnerabilidad de ejecución remota de código en tiempo de ejecución remota de llamada a procedimiento remoto	Importante	No	No	8.1
CVE-2023-24869	Vulnerabilidad de ejecución remota de código en tiempo de ejecución remota de llamada a procedimiento remoto	Importante	No	No	8.1
CVE-2023-23399	Vulnerabilidad de ejecución remota de código en Microsoft Excel	Importante	No	No	7.8

CVE-2023-24930	Vulnerabilidad de elevación de privilegios en Microsoft OneDrive para MacOS	Importante	No	No	7.8
CVE-2023-23401	Vulnerabilidad de ejecución remota de código en Windows Media	Importante	No	No	7.8
CVE-2023-23402	Vulnerabilidad de ejecución remota de código en Windows Media	Importante	No	No	7.8
CVE-2023-23410	Vulnerabilidad de elevación de privilegios en Windows HTTP.sys	Importante	No	No	7.8
CVE-2023-23412	Vulnerabilidad de elevación de privilegios en la imagen de cuentas de Windows	Importante	No	No	7.8
CVE-2023-23417	Vulnerabilidad de elevación de privilegios en el controlador de administración de particiones de Windows	Importante	No	No	7.8
CVE-2023-23418	Vulnerabilidad de elevación de privilegios del Sistema de archivos resistente a Windows (ReFS)	Importante	No	No	7.8
CVE-2023-23419	Vulnerabilidad de elevación de privilegios del Sistema de archivos resistente a Windows (ReFS)	Importante	No	No	7.8
CVE-2023-23420	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8

CVE-2023-23421	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2023-23422	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2023-23423	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2023-24910	Vulnerabilidad de elevación de privilegios en componentes gráficos de Windows	Importante	No	No	7.8
CVE-2023-24859	Vulnerabilidad de denegación de servicio en la extensión de intercambio de claves Internet (IKE) en Windows	Importante	No	No	7.5
CVE-2023-23400	Vulnerabilidad de ejecución remota de código en el servidor DNS de Windows	Importante	No	No	7.2
CVE-2023-23398	Vulnerabilidad de suplantación de identidad en Microsoft Excel	Importante	No	No	7.1
CVE-2023-23407	Vulnerabilidad de ejecución remota de código en el protocolo punto a punto a través de Ethernet (PPPoE) en Windows	Importante	No	No	7.1
CVE-2023-23414	Vulnerabilidad de ejecución remota de código en el protocolo punto a punto a través de	Importante	No	No	7.1

	Ethernet (PPPoE) en Windows				
CVE-2023-24892	Vulnerabilidad de suplantación de identidad en Webview2 en Microsoft Edge (basado en Chromium)	Importante	No	No	7.1
CVE-2023-23385	Vulnerabilidad de elevación de privilegios del protocolo punto a punto a través de Ethernet (PPPoE) en Windows	Importante	No	No	7.0
CVE-2023-23393	Vulnerabilidad de elevación de privilegios en el servicio Windows BrokerInfrastructure	Importante	No	No	7.0
CVE-2023-24861	Vulnerabilidad de elevación de privilegios en componentes gráficos de Windows	Importante	No	No	7.0
CVE-2023-23396	Vulnerabilidad de denegación de servicio en Microsoft Excel	Importante	No	No	6.5
CVE-2023-24856	Vulnerabilidad de divulgación de información del controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	6.5
CVE-2023-24922	Vulnerabilidad de divulgación de información en Microsoft Dynamics 365	Importante	No	No	6.5
CVE-2023-24857	Vulnerabilidad de divulgación de información del controlador de	Importante	No	No	6.5

	impresora de clase PostScript y PCL6 de Microsoft				
CVE-2023-24858	Vulnerabilidad de divulgación de información del controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	6.5
CVE-2023-24863	Vulnerabilidad de divulgación de información del controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	6.5
CVE-2023-24865	Vulnerabilidad de divulgación de información del controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	6.5
CVE-2023-24866	Vulnerabilidad de divulgación de información del controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	6.5
CVE-2023-24906	Vulnerabilidad de divulgación de información del controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	6.5
CVE-2023-24870	Vulnerabilidad de divulgación de información del controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	6.5

CVE-2023-24911	Vulnerabilidad de divulgación de información del controlador de impresora de clase PostScript y PCL6 de Microsoft	Importante	No	No	6.5
CVE-2023-24890	Vulnerabilidad de omisión de característica de seguridad en Microsoft OneDrive para iOS	Importante	No	No	6.5
CVE-2023-23389	Vulnerabilidad de elevación de privilegios en Microsoft Defender	Importante	No	No	6.3
CVE-2023-23391	Vulnerabilidad de suplantación de identidad en Office para Android	Importante	No	No	5.5
CVE-2023-23394	Vulnerabilidad de divulgación de información del subsistema de tiempo de ejecución cliente-servidor (CSRSS)	Importante	No	No	5.5
CVE-2023-24923	Vulnerabilidad de divulgación de información en Microsoft OneDrive para Android	Importante	No	No	5.5
CVE-2023-24882	Vulnerabilidad de divulgación de información en Microsoft OneDrive para Android	Importante	No	No	5.5
CVE-2023-23409	Vulnerabilidad de divulgación de información del subsistema de tiempo de ejecución cliente-servidor (CSRSS)	Importante	No	No	5.5

CVE-2023-24862	Vulnerabilidad de denegación de servicio en el canal seguro de Windows	Importante	No	No	5.5
CVE-2023-24919	Vulnerabilidad de secuencias de comandos entre sitios en Microsoft Dynamics 365 (local)	Importante	No	No	5.4
CVE-2023-24879	Vulnerabilidad de secuencias de comandos entre sitios en Microsoft Dynamics 365 (local)	Importante	No	No	5.4
CVE-2023-24920	Vulnerabilidad de secuencias de comandos entre sitios en Microsoft Dynamics 365 (local)	Importante	No	No	5.4
CVE-2023-24891	Vulnerabilidad de secuencias de comandos entre sitios en Microsoft Dynamics 365 (local)	Importante	No	No	5.4
CVE-2023-23946	GitHub: vulnerabilidad de ejecución remota de código en mingit	Importante	No	No	5.4
CVE-2023-22743	GitHub: Vulnerabilidad de elevación de privilegios en Git para Windows Installer	Importante	No	No	5.4
CVE-2023-23618	GitHub: Vulnerabilidad de ejecución remota de código en Git para Windows	Importante	No	No	5.4
CVE-2023-23408	Vulnerabilidad de suplantación de identidad en Azure Apache Ambari	Importante	No	No	4.5

CVE-2023-24921	Vulnerabilidad de secuencias de comandos entre sitios en Microsoft Dynamics 365 (local)	Importante	No	No	4.1
CVE-2023-23395	Vulnerabilidad de suplantación de identidad en Microsoft SharePoint Server	Importante	No	No	3.1
CVE-2023-24880	Vulnerabilidad de omisión de la característica de seguridad SmartScreen de Windows	Moderada	Sí	Sí	5.4
CVE-2023-20032	Mariner	Sin valor asignado	No	No	9.8
CVE-2023-0567	Mariner	Sin valor asignado	No	No	6.2
CVE-2023-20052	Mariner	Sin valor asignado	No	No	5.3
CVE-2023-1213	Chromium: Use after free en Swiftshader	Sin valor asignado			
CVE-2023-1214	Chromium: Confusión de tipo en V8	Sin valor asignado			
CVE-2023-1215	Chromium: Confusión de tipo en CSS	Sin valor asignado			
CVE-2023-1216	Chromium: Use after free en DevTools	Sin valor asignado			
CVE-2023-1217	Chromium: Desbordamiento del búfer de pila en los informes de fallos	Sin valor asignado			
CVE-2023-1218	Chromium: Use after free en WebRTC	Sin valor asignado			

CVE-2023-1219	Chromium: Desbordamiento del búfer del montón en Métricas	Sin valor asignado			
CVE-2023-1220	Chromium: Desbordamiento del búfer del montón en UMA	Sin valor asignado			
CVE-2023-1221	Chromium: Aplicación de directivas insuficiente en la API de extensiones	Sin valor asignado			
CVE-2023-1222	Chromium: Desbordamiento del búfer de montón en Web Audio API	Sin valor asignado			
CVE-2023-1223	Chromium: Aplicación insuficiente de directivas en Autorrelleno	Sin valor asignado			
CVE-2023-1224	Chromium: Aplicación insuficiente de directivas en la API de pagos web	Sin valor asignado			
CVE-2023-1228	Chromium: Aplicación insuficiente de políticas en Intents	Sin valor asignado			
CVE-2023-1229	Chromium: Implementación inadecuada en solicitudes de permisos	Sin valor asignado			
CVE-2023-1230	Chromium: Implementación inadecuada en instalaciones de WebApp	Sin valor asignado			
CVE-2023-1231	Chromium: Implementación inadecuada en Autorrelleno	Sin valor asignado			

CVE-2023-1232	Chromium: Aplicación insuficiente de directivas en la sincronización de recursos	Sin valor asignado			
CVE-2023-1233	Chromium: Aplicación insuficiente de directivas en la sincronización de recursos	Sin valor asignado			
CVE-2023-1234	Chromium: Implementación inadecuada en Intents	Sin valor asignado			
CVE-2023-1235	Chromium: Confusión de tipos en DevTools	Sin valor asignado			
CVE-2023-1236	Chromium: Implementación inadecuada en Internals	Sin valor asignado			

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 2023 Security Updates
- Security Update Guide - Microsoft
- Zero Day initiative-The March 2023 Security Update Review


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA