Basque CyberSecurity Centre

Actualización de seguridad de Microsoft-Junio 2023

BCSC-ACTUALIZACIONES-MICROSOFT-2023-JUNIO

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 junio de 2023 en las que se corrigen 94 vulnerabilidades, siendo 6 de ellas calificadas como críticas, 69 como importantes, 3 moderadas, 2 bajas y 14 sin un valor asignado. Estas últimas corrigen problemas en el navegador Edge basado en Chromium.

Estas vulnerabilidades afectan a productos como Microsoft SharePoint Server, Windows PGM, .NET, .NET Framework, Visual Studio, Microsoft Office OneNote, Microsoft Windows Codecs Library, Windows NTFS, Windows Group Policy y Remote Desktop Client entre otros.

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

- 26 vulnerabilidades de ejecución remota de código.
- 18 vulnerabilidades de elevación de privilegios.
- 10 vulnerabilidades de denegación de servicio.
- 9 vulnerabilidades de spoofing.
- 5 vulnerabilidades que afectan a Github.
- 5 vulnerabilidades de divulgación de información.
- 4 vulnerabilidades de bypass
- 4 vulnerabilidades Use After Free.
- 4 vulnerabilidades de implementación inadecuada.
- 4 vulnerabilidades implementación inadecuada.
- 3 vulnerabilidades de confusión de tipos.
- 1 vulnerabilidad de validación de datos insuficiente.
- 1 vulnerabilidad de desbordamiento del búfer de pila.

2. Recursos afectados

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

- Azure DevOps
- .NET and Visual Studio
- Microsoft Dynamics
- Windows CryptoAPI
- Microsoft Exchange Server
- .NET Framework
- .NET Core
- NuGet Client
- Microsoft Edge (basado en Chromium)
- Windows NTFS
- Windows Group Policy
- Remote Desktop Client
- SysInternals
- Windows DHCP Server
- Microsoft Office SharePoint
- Windows GDI
- Windows Win32K
- Windows TPM Device Driver
- Windows Cloud Files Mini Filter Driver
- Remote Desktop Client
- Windows PGM
- Windows Authentication Methods
- Microsoft Windows Codecs Library
- Windows Geolocation Service
- Windows OLE
- Windows Filtering
- Windows Remote Procedure Call Runtime
- Microsoft Windows Codecs Library

- Microsoft WDAC OLE DB provider for SQL
- Windows ODBC Driver
- Windows Resilient File System (ReFS)
- Windows Collaborative Translation Framework
- Windows Bus Filter Driver
- Windows iSCSI
- Windows Container Manager Service
- Windows Hyper-V
- Windows Installer
- Microsoft Printer Drivers
- Windows Hello
- Windows Kernel
- Role: DNS Server
- Windows SMB
- Windows Server Service
- Microsoft Power Apps
- Microsoft Office Excel
- Microsoft Exchange Server
- Microsoft Office SharePoint
- Microsoft Office Outlook
- Visual Studio
- Microsoft Office OneNote
- ASP .NET
- Microsoft Office SharePoint

3. Análisis técnico

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

CVE-2023-29357: vulnerabilidad de elevación de privilegios en Microsoft SharePoint Server. Un atacante que aprovechara esta vulnerabilidad podría obtener privilegios de administrador, de forma que, si ha obtenido acceso a tokens de autenticación JWT falsificados puede usarlos para ejecutar un ataque de red que omite la autenticación y le permite obtener acceso a los privilegios de un usuario autenticado. El atacante no necesita privilegios ni necesita realizar ninguna acción.

TTP

- Táctica TA0008 – Lateral Movement
- Técnica T1210 – Exploitation of Remote Services
- Técnica T1550.001 – Use Alternate Authentication Material: Application Access Token
- Táctica TA0009 – Collection
- Técnica T1213.002– Data from Information Repositories: Sharepoint

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-2023-29363: vulnerabilidad de ejecución remota de código en la multidifusión general (PGM) de Windows. Cuando el servicio de cola de mensajes de Windows se ejecuta en un entorno de PGM Server, un atacante podría enviar un archivo especialmente diseñado a través de la red para lograr la ejecución remota de código e intentar activar código malintencionado.

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-2023-32014: vulnerabilidad de ejecución remota de código en la multidifusión general (PGM) de Windows. Cuando el servicio de cola de mensajes de Windows se ejecuta en un entorno de PGM Server, un atacante podría enviar un archivo especialmente diseñado a través de la red para lograr la ejecución remota de código e intentar activar código malintencionado.

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-2023-32015: vulnerabilidad de ejecución remota de código en la multidifusión general (PGM) de Windows. Cuando el servicio de cola de mensajes de Windows se ejecuta en un entorno de PGM Server, un atacante podría enviar un archivo especialmente diseñado a través de la red para lograr la ejecución remota de código e intentar activar código malintencionado.

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-2023-24897: vulnerabilidad de ejecución remota de código en .NET, .NET Framework y Visual Studio.

TTP

- Táctica TA0002 – Execution
- Técnica T1059– Command and Scripting Interpreter
- Técnica T1050.005 – Command and Scripting Interpreter: Visual Basic

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.8

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

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

CVE-2023-32013: vulnerabilidad de denegación de servicio en Windows Hyper-V.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 6.5

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

- **Vector de ataque**: **Red**
- **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 representan a aquellas que se conoce que están siendo explotadas o que tienen el potencial de serlo, en función del estado de la amenaza. Estas vulnerabilidades se

encuentran presentes en la última versión del software suministrada por el fabricante.

CVE	Descripción	Severidad	Divulgado	Explotado	CVSS	Soluciones alternativas
CVE-2023-29357*	Vulnerabilidad de elevación de privilegios en Microsoft SharePoint Server	**Crítica**	No	No	9.8	Sí
CVE-2023-29363	Vulnerabilidad de ejecución remota de código en la multidifusión general (PGM) de Windows	**Crítica**	No	No	9.8	Sí
CVE-2023-32014	Vulnerabilidad de ejecución remota de código en la multidifusión general (PGM) de Windows	**Crítica**	No	No	9.8	Sí
CVE-2023-32015	Vulnerabilidad de ejecución remota de código en la multidifusión general (PGM) de Windows	**Crítica**	No	No	9.8	Sí
CVE-2023-24897	Vulnerabilidad de ejecución remota de código en .NET, .NET Framework y Visual Studio	**Crítica**	No	No	7.8	No
CVE-2023-32013	Vulnerabilidad de denegación de servicio en Windows Hyper-V	**Crítica**	No	No	6.5	No
CVE-2023-32031*	Vulnerabilidad de ejecución remota de	Importante	No	No	8.8	No

	código en Microsoft Exchange Server					
CVE-2023-29362	Vulnerabilidad de ejecución remota de código en el cliente de Escritorio remoto	Importante	No	No	8.8	No
CVE-2023-29372	Vulnerabilidad de ejecución remota de código en el proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8	No
CVE-2023-29373	Vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft	Importante	No	No	8.8	No
CVE-2023-32009	Vulnerabilidad de elevación de privilegios en el marco de traducción colaborativa de Windows	Importante	No	No	8.8	No
CVE-2023-33131	Vulnerabilidad de ejecución remota de código en Microsoft Outlook	Importante	No	No	8.8	No
CVE-2023-29351	Vulnerabilidad de elevación de privilegios en la directiva de grupo de Windows	Importante	No	No	8.1	No

CVE-2023-28310*	Vulnerabilidad de ejecución remota de código en Microsoft Exchange Server	Importante	No	No	8.0	No
CVE-2023-29326	Vulnerabilidad de ejecución remota de código en .NET Framework	Importante	No	No	7.8	No
CVE-2023-32029	Vulnerabilidad de ejecución remota de código en Microsoft Excel	Importante	No	No	7.8	No
CVE-2023-33137	Vulnerabilidad de ejecución remota de código en Microsoft Excel	Importante	No	No	7.8	No
CVE-2023-33146	Vulnerabilidad de ejecución remota de código en Microsoft Office	Importante	No	No	7.8	No
CVE-2023-24895	Vulnerabilidad de ejecución remota de código en .NET, .NET Framework y Visual Studio	Importante	No	No	7.8	No
CVE-2023-29346	Vulnerabilidad de elevación de privilegios NTFS	Importante	No	No	7.8	No
CVE-2023-29358*	Vulnerabilidad de elevación de privilegios en la GDI de Windows	Importante	No	No	7.8	No
CVE-2023-29359*	Vulnerabilidad de elevación de privilegios en GDI	Importante	No	No	7.8	No

CVE-2023-29360*	Vulnerabilidad de elevación de privilegios en el controlador de dispositivo TPM de Windows	Importante	No	No	7.8	No
CVE-2023-29365	Vulnerabilidad de ejecución remota de código en Windows Media	Importante	No	No	7.8	No
CVE-2023-29366	Vulnerabilidad de ejecución remota de código en el servicio de geolocalización de Windows	Importante	No	No	7.8	No
CVE-2023-29367	Vulnerabilidad de ejecución remota de código en el proveedor WMI de destino iSCSI	Importante	No	No	7.8	No
CVE-2023-29370	Vulnerabilidad de ejecución remota de código en Windows Media	Importante	No	No	7.8	No
CVE-2023-29371*	Vulnerabilidad de elevación de privilegios en la GDI de Windows	Importante	No	No	7.8	No
CVE-2023-32008	Vulnerabilidad de ejecución remota de código en el Sistema de archivos resistente a Windows (ReFS)	Importante	No	No	7.8	No
CVE-2023-32017	Vulnerabilidad de ejecución remota de código en el controlador de	Importante	No	No	7.8	No

	impresora PostScript de Microsoft					
CVE-2023-32018	Vulnerabilidad de ejecución remota de código en Windows Hello	Importante	No	No	7.8	No
CVE-2023-33133	Vulnerabilidad de ejecución remota de código en Microsoft Excel	Importante	No	No	7.8	No
CVE-2023-32022	Vulnerabilidad de omisión de la característica de seguridad del servicio de Windows Server	Importante	No	No	7.6	Sí
CVE-2023-29331	Vulnerabilidad de denegación de servicio en .NET, .NET Framework y Visual Studio	Importante	No	No	7.5	No
CVE-2023-32011	Vulnerabilidad de denegación de servicio en el servicio de detección iSCSI en Windows	Importante	No	No	7.5	No
CVE-2023-32030	Vulnerabilidad de denegación de servicio en .NET y Visual Studio	Importante	No	No	7.5	No
CVE-2023-33141	Vulnerabilidad de denegación de servicio de proxy inverso (YARP)	Importante	No	No	7.5	No
CVE-2023-33126	Vulnerabilidad de ejecución remota de código en .NET y Visual Studio	Importante	No	No	7.3	No

CVE-2023-33128	Vulnerabilidad de ejecución remota de código en .NET y Visual Studio	Importante	No	No	7.3	No
CVE-2023-33130	Vulnerabilidad de suplantación de identidad en Microsoft SharePoint Server	Importante	No	No	7.3	No
CVE-2023-33135	Vulnerabilidad de elevación de privilegios en .NET y Visual Studio	Importante	No	No	7.3	No
CVE-2023-27909	AutoDesk: Vulnerabilidad de escritura fuera de límites en Autodesk® FBX® SDK 2020 o anterior	Importante	No	No	7.3	No
CVE-2023-27910	AutoDesk: vulnerabilidad de desbordamiento de búfer de pila en Autodesk® FBX® SDK 2020 o anterior	Importante	No	No	7.3	No
CVE-2023-27911	AutoDesk: vulnerabilidad de desbordamiento del búfer del montón en Autodesk® FBX® SDK 2020 o versiones anteriores	Importante	No	No	7.3	No
CVE-2023-21565	Vulnerabilidad de suplantación de identidad en Azure DevOps Server	Importante	No	No	7.1	No

CVE-2023-29337	Vulnerabilidad de ejecución remota de código en el cliente NuGet	Importante	No	No	7.1	No
CVE-2023-29012	GitHub: Git CMD ejecuta erróneamente 'doskey.exe' en el directorio actual, si existe	Importante	No	No	7.1	No
CVE-2023-29011	GitHub: El archivo de configuración de 'connect.exe' es susceptible de colocación maliciosa	Importante	No	No	7.1	No
CVE-2023-25815	GitHub: Git busca mensajes localizados en un lugar sin privilegios	Importante	No	No	7.1	No
CVE-2023-29007	GitHub: Inyección de configuración arbitraria a través de 'git submodule deinit'	Importante	No	No	7.1	No
CVE-2023-25652	GitHub: "git apply --reject" escritura de archivos arbitrarios parcialmente controlada	Importante	No	No	7.1	No
CVE-2023-32021	Vulnerabilidad de omisión de la característica de seguridad del servicio testigo SMB de Windows	Importante	No	No	7.1	Sí
CVE-2023-29361*	Vulnerabilidad de elevación de privilegios en el	Importante	No	No	7.0	No

	controlador de minifiltro de archivos de nube de Windows					
CVE-2023-29364	Vulnerabilidad de elevación de privilegios en la autenticación de Windows	Importante	No	No	7.0	No
CVE-2023-29368	Vulnerabilidad de elevación de privilegios en la plataforma de filtrado de Windows	Importante	No	No	7.0	No
CVE-2023-32010	Vulnerabilidad de elevación de privilegios en el controlador de filtro de bus de Windows	Importante	No	No	7.0	No
CVE-2023-24937	Vulnerabilidad de denegación de servicio de Windows CryptoAPI	Importante	No	No	6.5	No
CVE-2023-24938	Vulnerabilidad de denegación de servicio de Windows CryptoAPI	Importante	No	No	6.5	No
CVE-2023-29352	Vulnerabilidad de omisión de la característica de seguridad de Escritorio remoto de Windows	Importante	No	No	6.5	No
CVE-2023-29369	Vulnerabilidad de denegación de servicio en tiempo de ejecución en tiempo de ejecución de llamada a	Importante	No	No	6.5	No

	procedimiento remoto					
CVE-2023-32032	Vulnerabilidad de elevación de privilegios en .NET y Visual Studio	Importante	No	No	6.5	No
CVE-2023-33129	Vulnerabilidad de denegación de servicio en Microsoft SharePoint	Importante	No	No	6.5	No
CVE-2023-33140	Vulnerabilidad de suplantación de identidad en Microsoft OneNote	Importante	No	No	6.5	No
CVE-2023-33142	Vulnerabilidad de elevación de privilegios en Microsoft SharePoint Server	Importante	No	No	6.5	No
CVE-2023-33145	Vulnerabilidad de divulgación de información en Microsoft Edge (basado en Chromium)	Importante	No	No	6.5	No
CVE-2023-32012	Vulnerabilidad de elevación de privilegios en el servicio Administrador de contenedores de Windows	Importante	No	No	6.3	No
CVE-2023-33132	Vulnerabilidad de suplantación de identidad en Microsoft SharePoint Server	Importante	No	No	6.3	No
CVE-2023-33139	Vulnerabilidad de divulgación de información en Visual Studio	Importante	No	No	5.5	No

CVE-2023-32016	Vulnerabilidad de divulgación de información en Windows Installer	Importante	No	No	5.5	No
CVE-2023-24896	Vulnerabilidad de suplantación de identidad en Dynamics 365 Finance	Importante	No	No	5.4	No
CVE-2023-29355	Vulnerabilidad de divulgación de información en el servicio del servidor DHCP	Importante	No	No	5.3	Sí
CVE-2023-33144	Vulnerabilidad de suplantación de código en Visual Studio	Importante	No	No	5.0	No
CVE-2023-32019	Vulnerabilidad de divulgación de información en el kernel de Windows	Importante	No	No	4.7	No
CVE-2023-32020	Vulnerabilidad de suplantación de DNS en Windows	Importante	No	No	3.7	No
CVE-2023-32024	Vulnerabilidad de suplantación de identidad en Microsoft Power Apps	Importante	No	No	3.0	No
CVE-2023-24936	Vulnerabilidad de elevación de privilegios en .NET, .NET Framework y Visual Studio	Moderada	No	No	8.1	No
CVE-2023-33143	Vulnerabilidad de elevación de privilegios en Microsoft Edge (basado en Chromium)	Moderada	No	No	7.5	No

CVE-2023-21569	Vulnerabilidad de suplantación de identidad en Azure DevOps Server	Moderada	No	No	5.5	No
CVE-2023-29345	Vulnerabilidad de omisión de característica de seguridad en Microsoft Edge (basado en Chromium)	Baja	No	No	6.1	No
CVE-2023-29353	Vulnerabilidad de denegación de servicio en Sysinternals Process Monitor for Windows	Baja	No	No	5.5	No
CVE-2023-2929	Chromium: Escritura fuera de límites en Swiftshader	Sin valor asignado	No	No	6.5	No
CVE-2023-2930	Chromium: Use after free en Extensions	Sin valor asignado	No	No	6.5	No
CVE-2023-2931	Chromium: Use after free en PDF	Sin valor asignado	No	No	6.5	No
CVE-2023-2932	Chromium: Use after free en PDF	Sin valor asignado	No	No	6.5	No
CVE-2023-2933	Chromium: Use after free en PDF	Sin valor asignado	No	No	6.5	No
CVE-2023-2934	Chromium: Acceso a memoria fuera de límites en Mojo	Sin valor asignado	No	No	6.5	No
CVE-2023-2935	Chromium: Confusión de tipo en V8	Sin valor asignado	No	No	6.5	No
CVE-2023-2936	Chromium: Confusión de tipo en V8	Sin valor asignado	No	No	6.5	No

CVE-2023-2937	Chromium: Aplicación inadecuada en Picture In Picture	Sin valor asignado	No	No	6.5	No
CVE-2023-2938	Chromium: Aplicación inadecuada en Picture In Picture	Sin valor asignado	No	No	6.5	No
CVE-2023-2939	Chromium: Validación de datos insuficiente en Installer	Sin valor asignado	No	No	6.5	No
CVE-2023-2940	Chromium: Aplicación inadecuada en Downloads	Sin valor asignado	No	No	6.5	No
CVE-2023-2941	Chromium: Aplicación inadecuada en Extensions API	Sin valor asignado	No	No	6.5	No
CVE-2023-3079	Chromium: Confusión de tipos en V8	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

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


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA