

Actualización de seguridad de Microsoft-Septiembre 2023

BCSC-ACTUALIZACIONES-MICROSOFT-2023-
SEPTIEMBRE

TLP: CLEAR

www.ciberseguridad.eus



TABLA DE CONTENIDO

Sobre el BCSC.....	3
1. Resumen ejecutivo.....	4
2. Recursos afectados.....	5
3. Análisis técnico.....	6
4. Mitigación / Solución.....	14
5. Referencias Adicionales.....	14

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 Respuesta 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:



1. Resumen ejecutivo

Microsoft ha publicado las actualizaciones de seguridad del mes de septiembre de 2023 en las que se corrigen 66 vulnerabilidades, siendo 2 de ellas calificadas como críticas, 58 como importantes, 1 moderada y 5 sin un valor asignado que corrigen problemas en el navegador Edge basado en Chromium.

2. Recursos afectados

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

- Microsoft Azure Kubernetes Service
- Azure DevOps
- Windows Cloud Files Mini Filter Driver
- Microsoft Identity Linux Broker
- 3D Viewer
- Visual Studio Code
- Microsoft Exchange Server
- Visual Studio
- Microsoft Office Word , Outlook , Sharepoint & Excel
- 3D Builder
- .NET Framework
- .NET and Visual Studio
- .NET Core & Visual Studio
- Microsoft Dynamics Finance & Operations
- Windows DHCP Server
- Microsoft Streaming Service
- Windows Kernel
- Windows GDI
- Windows Scripting
- Microsoft Dynamics
- Windows Common Log File System Driver
- Windows Themes
- Microsoft Windows Codecs Library
- Windows Internet Connection Sharing (ICS)
- Windows TCP/IP
- Azure HDInsights
- Windows Defender

3. Análisis técnico

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

CVE-2023-38148: vulnerabilidad de ejecución remota de código en conexión compartida a Internet (ICS).

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.8

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

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

CVE-2023-29332: vulnerabilidad de elevación de privilegios del servicio Microsoft Azure Kubernetes.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.5

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

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

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.

CVE	Descripción	Severidad	Divulgado	Explotado	CVSS	Soluciones alternativas
CVE-2023-38148	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability	Crítica	No	No	8.8	Sí
CVE-2023-29332	Microsoft Azure Kubernetes Service Elevation of Privilege Vulnerability	Crítica	No	No	7.5	No
CVE-2023-38147	Windows Miracast Wireless Display Remote Code Execution Vulnerability	Importante	No	No	8.8	No
CVE-2023-38146	Windows Themes Remote Code Execution Vulnerability	Importante	No	No	8.8	No
CVE-2023-33136	Azure DevOps Server Remote Code Execution Vulnerability	Importante	No	No	8.8	No
CVE-2023-36764	Microsoft SharePoint Server Elevation of Privilege Vulnerability	Importante	No	No	8.8	No
CVE-2023-36757	Microsoft Exchange Server Spoofing Vulnerability	Importante	No	No	8.0	No
CVE-2023-36756	Microsoft Exchange Server Remote Code Execution Vulnerability	Importante	No	No	8.0	No
CVE-2023-36745	Microsoft Exchange Server Remote Code	Importante	No	No	8.0	No

	Execution Vulnerability					
CVE-2023-36744	Microsoft Exchange Server Remote Code Execution Vulnerability	Importante	No	No	8.0	No
CVE-2023-35355	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Importante	No	No	7.8	No
CVE-2023-38161	Windows GDI Elevation of Privilege Vulnerability	Importante	No	No	7.8	No
CVE-2023-38150	Windows Kernel Elevation of Privilege Vulnerability	Importante	No	No	7.8	No
CVE-2023-38144	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Importante	No	No	7.8	No
CVE-2023-38143	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Importante	No	No	7.8	No
CVE-2023-38142	Windows Kernel Elevation of Privilege Vulnerability	Importante	No	No	7.8	No
CVE-2023-38141	Windows Kernel Elevation of Privilege Vulnerability	Importante	No	No	7.8	No
CVE-2023-38139	Windows Kernel Elevation of Privilege Vulnerability	Importante	No	No	7.8	No
CVE-2023-36804	Windows GDI Elevation of	Importante	No	No	7.8	No

	Privilege Vulnerability					
CVE-2023-36802	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability	Importante	No	Sí	7.8	No
CVE-2023-36766	Microsoft Excel Information Disclosure Vulnerability	Importante	No	No	7.8	No
CVE-2023-36765	Microsoft Office Elevation of Privilege Vulnerability	Importante	No	No	7.8	No
CVE-2023-36758	Visual Studio Elevation of Privilege Vulnerability	Importante	No	No	7.8	No
CVE-2023-36742	Visual Studio Code Remote Code Execution Vulnerability	Importante	No	No	7.8	No
CVE-2023-38163	Windows Defender Attack Surface Reduction Security Feature Bypass	Importante	No	No	7.8	No
CVE-2023-36796	Visual Studio Remote Code Execution Vulnerability	Importante	No	No	7.8	No
CVE-2023-36794	Visual Studio Remote Code Execution Vulnerability	Importante	No	No	7.8	No
CVE-2023-36793	Visual Studio Remote Code Execution Vulnerability	Importante	No	No	7.8	No
CVE-2023-36792	Visual Studio Remote Code Execution Vulnerability	Importante	No	No	7.8	No

CVE-2023-36788	.NET Framework Remote Code Execution Vulnerability	Importante	No	No	7.8	No
CVE-2023-36773	3D Builder Remote Code Execution Vulnerability	Importante	No	No	7.8	No
CVE-2023-36772	3D Builder Remote Code Execution Vulnerability	Importante	No	No	7.8	No
CVE-2023-36771	3D Builder Remote Code Execution Vulnerability	Importante	No	No	7.8	No
CVE-2023-36770	3D Builder Remote Code Execution Vulnerability	Importante	No	No	7.8	No
CVE-2023-36760	3D Viewer Remote Code Execution Vulnerability	Importante	No	No	7.8	No
CVE-2023-39956	Electron: CVE-2023-39956 - Visual Studio Code Remote Code Execution Vulnerability	Importante	No	No	7.8	No
CVE-2023-36740	3D Viewer Remote Code Execution Vulnerability	Importante	No	No	7.8	No
CVE-2023-36739	3D Viewer Remote Code Execution Vulnerability	Importante	No	No	7.8	No
CVE-2023-36886	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	Importante	No	No	7.6	No
CVE-2023-38164	Microsoft Dynamics 365 (on-premises)	Importante	No	No	7.6	No

	Cross-site Scripting Vulnerability					
CVE-2023-36800	Dynamics Finance and Operations Cross-site Scripting Vulnerability	Importante	No	No	7.6	No
CVE-2023-38162	DHCP Server Service Denial of Service Vulnerability	Importante	No	No	7.5	Sí
CVE-2023-38149	Windows TCP/IP Denial of Service Vulnerability	Importante	No	No	7.5	Sí
CVE-2023-36763	Microsoft Outlook Information Disclosure Vulnerability	Importante	No	No	7.5	No
CVE-2023-36762	Microsoft Word Remote Code Execution Vulnerability	Importante	No	No	7.3	No
CVE-2023-38156	Azure HDInsight Apache Ambari Elevation of Privilege Vulnerability	Importante	No	No	7.2	No
CVE-2023-36805	Windows MSHTML Platform Security Feature Bypass Vulnerability	Importante	No	No	7.0	No
CVE-2023-38155	Azure DevOps Server Remote Code Execution Vulnerability	Importante	No	No	7.0	No
CVE-2023-36759	Visual Studio Elevation of Privilege Vulnerability	Importante	No	No	6.7	No
CVE-2023-36799	.NET Core and Visual Studio	Importante	No	No	6.5	No

	Denial of Service Vulnerability					
CVE-2023-36761	Microsoft Word Information Disclosure Vulnerability	Importante	Sí	Sí	6.2	No
CVE-2023-36777	Microsoft Exchange Server Information Disclosure Vulnerability	Importante	No	No	5.7	No
CVE-2023-38140	Windows Kernel Information Disclosure Vulnerability	Importante	No	No	5.5	No
CVE-2023-36803	Windows Kernel Information Disclosure Vulnerability	Importante	No	No	5.5	No
CVE-2022-41303	AutoDesk: CVE-2022-41303 use-after-free vulnerability in Autodesk® FBX® SDK 2020 or prior	Importante	No	No	5.5	No
CVE-2023-38160	Windows TCP/IP Information Disclosure Vulnerability	Importante	No	No	5.5	No
CVE-2023-38152	DHCP Server Service Information Disclosure Vulnerability	Importante	No	No	5.3	Sí
CVE-2023-36801	DHCP Server Service Information Disclosure Vulnerability	Importante	No	No	5.3	Sí
CVE-2023-36736	Microsoft Identity Linux Broker Remote Code Execution Vulnerability	Importante	No	No	4.4	No

CVE-2023-36767	Microsoft Office Security Feature Bypass Vulnerability	Importante	No	No	4.3	No
CVE-2023-41764	Microsoft Office Spoofing Vulnerability	Moderada	No	No	5.5	No
CVE-2023-4863	Chromium: CVE-2023-4863 Heap buffer overflow in WebP	Sin valor asignado	No	No	7.8	No
CVE-2023-4761	Chromium: CVE-2023-4761 Out of bounds memory access in FedCM	Sin valor asignado				No
CVE-2023-4762	Chromium: CVE-2023-4762 Type Confusion in V8	Sin valor asignado				No
CVE-2023-4763	Chromium: CVE-2023-4763 Use after free in Networks	Sin valor asignado				No
CVE-2023-4764	Chromium: CVE-2023-4764 Incorrect security UI in BFCache	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

- [September 2023 Security Updates](#).
- [Security Update Guide - Microsoft](#).

