Basque CyberSecurity Centre

# Actualización de seguridad de Microsoft-Febrero 2023

BCSC-ACTUALIZACIONES-MICROSOFT-2023-FEBRERO

**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 febrero de 2023. Con estas actualizaciones se corrigen 80 vulnerabilidades, siendo 8 de ellas calificadas como críticas, 67 como importantes, 1 moderada, 2 bajas y 2 sin un valor asignado.

Dentro de ellas hay **3 vulnerabilidades zero-day, todas siendo explotadas,** cuyos identificadores son CVE-2023-21823, CVE-2023-23376, CVE-2023-21715.

Estas vulnerabilidades afectan a productos como Microsoft Graphics Component, Windows Active Directory, Windows Common Log File System Driver, Windows Kerberos, Visual Studio, Microsoft Office, Microsoft Office OneNote, Microsoft Office Publisher, Microsoft Office SharePoint y Microsoft Office Word entre otros.

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

- 2 vulnerabilidad de bypass.
- 10 vulnerabilidades de denegación de servicio.
- 8 vulnerabilidades de divulgación de información.
- 38 vulnerabilidades de ejecución remota de código.
- 11 vulnerabilidades de elevación de privilegios.
- 3 vulnerabilidades de spoofing.
- 1 vulnerabilidad de manipulación (Tampering).
- 6 vulnerabilidades de Cross-site Scripting (XSS).
- 1 vulnerabilidad de Use-After-Free en curl.

## 2. Recursos afectados

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

- .NET and Visual Studio
- .NET Framework
- 3D Builder
- Azure App Service
- Azure Data Box Gateway
- Azure DevOps
- Azure Machine Learning
- HoloLens
- Internet Storage Name Service
- Microsoft Defender for Endpoint
- Microsoft Defender for IoT
- Microsoft Dynamics
- Microsoft Edge (basado en Chromium)
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office OneNote
- Microsoft Office Publisher
- Microsoft Office SharePoint
- Microsoft Office Word
- Microsoft PostScript Printer Driver
- Microsoft WDAC OLE DB provider para SQL
- Microsoft Windows Codecs Library
- Power BI
- SQL Server
- Visual Studio
- Windows Active Directory
- Windows ALPC

- Windows Common Log File System Driver
- Windows Cryptographic Services
- Windows Distributed File System (DFS)
- Windows Fax and Scan Service
- Windows HTTP.sys
- Windows Installer
- Windows iSCSI
- Windows Kerberos
- Windows MSHTML Platform
- Windows ODBC Driver
- Windows Protected EAP (PEAP)
- Windows SChannel
- Windows Win32K

## 3. Análisis técnico

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

**Las 3 vulnerabilidades zero-day que están siendo explotadas son**:

CVE-2023-21823: vulnerabilidad de ejecución remota de código en el componente de gráficos de Windows.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.8

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-2023-23376: vulnerabilidad de elevación de privilegios en el controlador del sistema de archivos de registro común de Windows, de forma que un atacante que aprovechara esta vulnerabilidad podría obtener privilegios SYSTEM.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.8

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-2023-21715: vulnerabilidad de bypass de características de seguridad de Microsoft Publisher, de manera que un atacante que aprovechara esta vulnerabilidad podría omitir las directivas de macros de Office usadas para bloquear archivos malintencionados o que no son de confianza.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.3

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

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

Las vulnerabilidades críticas corregidas son:

CVE-2023-21803: vulnerabilidad de ejecución remota de código en el Servicio de detección iSCSI de Windows. Un atacante podría aprovechar la vulnerabilidad si envía una solicitud de detección DHCP malintencionada especialmente diseñada al servicio de detección iSCSI en equipos de 32 bits. Un atacante que aprovechara la vulnerabilidad podría obtener la capacidad de ejecutar código en el sistema de destino.

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-2023-21689: vulnerabilidad de ejecución remota de código en el Protocolo de autenticación extensible protegida (PEAP) de Microsoft, de manera que el atacante de esta vulnerabilidad podría dirigirse a las cuentas de servidor en una ejecución de código arbitraria o remota e intentar desencadenar código malintencionado en el contexto de la cuenta del servidor a través de una llamada de red. El atacante no necesita privilegios ni el usuario víctima necesita realizar ninguna acción.

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-2023-21690: vulnerabilidad de ejecución remota de código en el Protocolo de autenticación extensible protegida (PEAP) de Microsoft. Un atacante no autenticado podría atacar un servidor de Protocolo de autenticación extensible protegido (PEAP) de Microsoft enviando paquetes PEAP malintencionados especialmente diseñados a través de la red.

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-2023-21692: vulnerabilidad de ejecución remota de código en el Protocolo de autenticación extensible protegida (PEAP) de Microsoft. Un atacante no autenticado podría atacar un servidor de Protocolo de autenticación extensible protegido (PEAP) de Microsoft enviando paquetes PEAP malintencionados especialmente diseñados a través de la red.

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-2023-21716: vulnerabilidad de ejecución remota de código en Microsoft Word de forma que, un atacante no autenticado podría enviar un correo electrónico malintencionado que contuviera una carga RTF que le permitiría obtener acceso para ejecutar comandos dentro de la aplicación utilizada para abrir el archivo 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-2023-21815: vulnerabilidad de ejecución remota de código en Visual Studio.

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-2023-23381: vulnerabilidad de ejecución remota de código en Visual Studio.

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-2023-21718: vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft SQL. Un atacante podría aprovechar la vulnerabilidad engañando a un usuario no autenticado para que intentara conectarse a una base de datos malintencionada de SQL Server a través de ODBC. Esto podría provocar que la base de datos devuelva datos malintencionados que podrían provocar la ejecución de código arbitrario en el cliente.

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**

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

| CVE | Descripción | Severidad | Divulgado | Explotado | CVSS |
|---|---|---|---|---|---|
| CVE-2023-21803 | Vulnerabilidad de ejecución remota de código en el Servicio de detección iSCSI de Windows | **Crítica** | No | No | 9.8 |
| CVE-2023-21689 | Vulnerabilidad de ejecución remota de código en el Protocolo de autenticación extensible protegida (PEAP) de Microsoft | **Crítica** | No | No | 9.8 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-21690 | Vulnerabilidad de ejecución remota de código en el Protocolo de autenticación extensible protegida (PEAP) de Microsoft | **Crítica** | No | No | 9.8 |
| CVE-2023-21692 | Vulnerabilidad de ejecución remota de código en el Protocolo de autenticación extensible protegida (PEAP) de Microsoft | **Crítica** | No | No | 9.8 |
| CVE-2023-21716 | Vulnerabilidad de ejecución remota de código en Microsoft Word | **Crítica** | No | No | 9.8 |
| CVE-2023-21815 | Vulnerabilidad de ejecución remota de código en Visual Studio | **Crítica** | No | No | 8.4 |
| CVE-2023-23381 | Vulnerabilidad de ejecución remota de código en Visual Studio | **Crítica** | No | No | 8.4 |
| CVE-2023-21718 | Vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft SQL | **Crítica** | No | No | 7.8 |
| CVE-2023-21684 | Vulnerabilidad de ejecución remota de código en el controlador de | Importante | No | No | 8.8 |

| | | | | | |
|---|---|---|---|---|---|
| | impresora PostScript de Microsoft | | | | |
| CVE-2023-21705 | Vulnerabilidad de ejecución remota de código en Microsoft SQL Server | Importante | No | No | 8.8 |
| CVE-2023-21706 | Vulnerabilidad de ejecución remota de código en Microsoft Exchange Server | Importante | No | No | 8.8 |
| CVE-2023-21707 | Vulnerabilidad de ejecución remota de código en Microsoft Exchange Server | Importante | No | No | 8.8 |
| CVE-2023-21529 | Vulnerabilidad de ejecución remota de código en Microsoft Exchange Server | Importante | No | No | 8.8 |
| CVE-2023-21797 | Vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft | Importante | No | No | 8.8 |
| CVE-2023-21798 | Vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft | Importante | No | No | 8.8 |
| CVE-2023-21799 | Vulnerabilidad de ejecución remota de código en el proveedor OLE DB de Microsoft | Importante | No | No | 8.8 |

| | | | | | |
|---|---|---|---|---|---|
| | WDAC para SQL Server | | | | |
| CVE-2023-21685 | Vulnerabilidad de ejecución remota de código en el proveedor OLE DB de Microsoft WDAC para SQL Server | Importante | No | No | 8.8 |
| CVE-2023-21686 | Vulnerabilidad de ejecución remota de código en el proveedor OLE DB de Microsoft WDAC para SQL Server | Importante | No | No | 8.8 |
| CVE-2023-21713 | Vulnerabilidad de ejecución remota de código en Microsoft SQL Server | Importante | No | No | 8.8 |
| CVE-2023-21717 | Vulnerabilidad de elevación de privilegios en Microsoft SharePoint Server | Importante | No | No | 8.8 |
| CVE-2023-21777 | Vulnerabilidad de elevación de privilegios en Azure App Service en Azure Stack Hub | Importante | No | No | 8.7 |
| CVE-2023-21778 | Vulnerabilidad de ejecución remota de código en Microsoft Dynamics Unified Service Desk | Importante | No | No | 8.3 |
| CVE-2023-21806 | Vulnerabilidad de suplantación de identidad del | Importante | No | No | 8.2 |

| | | | | | |
|---|---|---|---|---|---|
| | servidor de informes de Power BI | | | | |
| CVE-2023-21528 | Vulnerabilidad de ejecución remota de código en Microsoft SQL Server | Importante | No | No | 7.8 |
| CVE-2023-21704 | Vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft para SQL Server | Importante | No | No | 7.8 |
| CVE-2023-21566 | Vulnerabilidad de elevación de privilegios en Visual Studio | Importante | No | No | 7.8 |
| CVE-2023-23378 | Vulnerabilidad de ejecución remota de código en Print 3D | Importante | No | No | 7.8 |
| CVE-2023-21800 | Vulnerabilidad de elevación de privilegios en Windows Installer | Importante | No | No | 7.8 |
| CVE-2023-21801 | Vulnerabilidad de ejecución remota de código en el controlador de impresora PostScript de Microsoft | Importante | No | No | 7.8 |
| CVE-2023-21802 | Vulnerabilidad de ejecución remota de código en Windows Media | Importante | No | No | 7.8 |
| CVE-2023-21804 | Vulnerabilidad de elevación de privilegios en | Importante | No | No | 7.8 |

| | | | | | |
|---|---|---|---|---|---|
| | componentes gráficos de Windows | | | | |
| CVE-2023-21805 | Vulnerabilidad de ejecución remota de código en la plataforma MSHTML de Windows | Importante | No | No | 7.8 |
| CVE-2023-21808 | Vulnerabilidad de ejecución remota de código en .NET y Visual Studio | Importante | No | No | 7.8 |
| CVE-2023-21809 | Vulnerabilidad de omisión de característica de Microsoft Defender para endpoint Security | Importante | No | No | 7.8 |
| CVE-2023-21812 | Vulnerabilidad de elevación de privilegios en el controlador del sistema de archivos de registro común de Windows | Importante | No | No | 7.8 |
| CVE-2023-21817 | Vulnerabilidad de elevación de privilegios Kerberos en Windows | Importante | No | No | 7.8 |
| CVE-2023-21822 | Vulnerabilidad de elevación de privilegios en componentes gráficos de Windows | Importante | No | No | 7.8 |
| CVE-2023-21823 | Vulnerabilidad de ejecución remota de código en el componente de | Importante | No | Sí | 7.8 |

| | | | | | |
|---|---|---|---|---|---|
| | gráficos de Windows | | | | |
| CVE-2023-21688 | Vulnerabilidad de elevación de privilegios en el kernel de NT OS | Importante | No | No | 7.8 |
| CVE-2023-23376 | Vulnerabilidad de elevación de privilegios en el controlador del sistema de archivos de registro común de Windows | Importante | No | Sí | 7.8 |
| CVE-2023-23377 | Vulnerabilidad de ejecución remota de código en 3D Builder | Importante | No | No | 7.8 |
| CVE-2023-23390 | Vulnerabilidad de ejecución remota de código en 3D Builder | Importante | No | No | 7.8 |
| CVE-2023-21553 | Vulnerabilidad de ejecución remota de código en Azure DevOps Server | Importante | No | No | 7.5 |
| CVE-2023-21811 | Vulnerabilidad de denegación de servicio en iSCSI en Windows | Importante | No | No | 7.5 |
| CVE-2023-21813 | Vulnerabilidad de denegación de servicio en el canal seguro de Windows | Importante | No | No | 7.5 |
| CVE-2023-21816 | Vulnerabilidad de denegación de servicio en la API de Servicios de dominio de Windows Active Directory | Importante | No | No | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-21818 | Vulnerabilidad de denegación de servicio en el canal seguro de Windows | Importante | No | No | 7.5 |
| CVE-2023-21819 | Vulnerabilidad de denegación de servicio en el canal seguro de Windows | Importante | No | No | 7.5 |
| CVE-2023-21691 | Vulnerabilidad de divulgación de información del Protocolo de autenticación extensible protegida (PEAP) de Microsoft | Importante | No | No | 7.5 |
| CVE-2023-21695 | Vulnerabilidad de ejecución remota de código en el Protocolo de autenticación extensible protegida (PEAP) de Microsoft | Importante | No | No | 7.5 |
| CVE-2023-21700 | Vulnerabilidad de denegación de servicio en el servicio de detección iSCSI en Windows | Importante | No | No | 7.5 |
| CVE-2023-21701 | Vulnerabilidad de denegación de servicio del Protocolo de autenticación extensible protegida (PEAP) de Microsoft | Importante | No | No | 7.5 |
| CVE-2023-21702 | Vulnerabilidad de denegación de servicio en | Importante | No | No | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| | iSCSI en Windows | | | | |
| CVE-2023-21820 | Vulnerabilidad de ejecución remota de código en el Sistema de archivos distribuido (DFS) de Windows | Importante | No | No | 7.4 |
| CVE-2023-21568 | Vulnerabilidad de ejecución remota de código en Microsoft SQL Server Integration Service (extensión VS) | Importante | No | No | 7.3 |
| CVE-2023-21715 | Vulnerabilidad de omisión de características de seguridad de Microsoft Publisher | Importante | No | Sí | 7.3 |
| CVE-2023-21710 | Vulnerabilidad de ejecución remota de código en Microsoft Exchange Server | Importante | No | No | 7.2 |
| CVE-2023-21564 | Vulnerabilidad de secuencias de comandos entre sitios en Azure DevOps Server | Importante | No | No | 7.1 |
| CVE-2023-21694 | Vulnerabilidad de ejecución remota de código en el servicio de fax de Windows | Importante | No | No | 6.8 |
| CVE-2023-21721 | Vulnerabilidad de suplantación de identidad en | Importante | No | No | 6.5 |

| | | | | | |
|---|---|---|---|---|---|
| | Microsoft OneNote | | | | |
| CVE-2023-21572 | Vulnerabilidad de secuencias de comandos entre sitios en Microsoft Dynamics 365 (local) | Importante | No | No | 6.5 |
| CVE-2023-23382 | Vulnerabilidad de divulgación de información de instancia de proceso de aprendizaje automático en Azure | Importante | No | No | 6.5 |
| CVE-2023-21703 | Vulnerabilidad de ejecución remota de código en Azure Data Box Gateway | Importante | No | No | 6.5 |
| CVE-2023-23379 | Vulnerabilidad de elevación de privilegios en Microsoft Defender para IoT | Importante | No | No | 6.4 |
| CVE-2023-21697 | Vulnerabilidad de divulgación de información del servidor del Servicio de nombres de almacenamiento en Internet (iSNS) en Windows | Importante | No | No | 6.2 |
| CVE-2023-21807 | Vulnerabilidad de secuencias de comandos entre sitios en Microsoft Dynamics 365 (local) | Importante | No | No | 5.8 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-21693 | Vulnerabilidad de divulgación de información del controlador de impresora PostScript de Microsoft | Importante | No | No | 5.7 |
| CVE-2023-21567 | Vulnerabilidad de denegación de servicio en Visual Studio | Importante | No | No | 5.6 |
| CVE-2023-21687 | Vulnerabilidad de divulgación de información en HTTP.sys | Importante | No | No | 5.5 |
| CVE-2023-21714 | Vulnerabilidad de divulgación de información en Microsoft Office | Importante | No | No | 5.5 |
| CVE-2023-21570 | Vulnerabilidad de secuencias de comandos entre sitios en Microsoft Dynamics 365 (local) | Importante | No | No | 5.4 |
| CVE-2023-21571 | Vulnerabilidad de secuencias de comandos entre sitios en Microsoft Dynamics 365 (local) | Importante | No | No | 5.4 |
| CVE-2023-21573 | Vulnerabilidad de secuencias de comandos entre sitios en Microsoft Dynamics 365 (local) | Importante | No | No | 5.4 |
| CVE-2023-21699 | Vulnerabilidad de divulgación de información del servidor del Servicio de nombres de | Importante | No | No | 5.3 |

| | | | | | |
|---|---|---|---|---|---|
| | almacenamiento en Internet (iSNS) en Windows | | | | |
| CVE-2023-21722 | Vulnerabilidad de denegación de servicio en .NET Framework | Importante | No | No | 4.4 |
| CVE-2023-23374 | Vulnerabilidad de ejecución remota de código en Microsoft Edge (basado en Chromium) | Moderada | No | No | 8.3 |
| CVE-2023-21720 | Vulnerabilidad de manipulación en Microsoft Edge (basado en Chromium) | Baja | No | No | 5.3 |
| CVE-2023-21794 | Vulnerabilidad de suplantación de identidad en Microsoft Edge (basado en Chromium) | Baja | No | No | 4.3 |
| CVE-2019-15126 | El tráfico específicamente temporizado y hecho a mano puede causar errores internos (relacionados con transiciones de estado) en un dispositivo WLAN | Sin valor asignado | No | No | 7.8 |
| CVE-2022-43552 | Mariner | Sin valor asignado | No | No | 7.8 |

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


EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA