Basque CyberSecurity Centre

# Actualización de seguridad de Microsoft-Noviembre 2022

BCSC-ACTUALIZACIONES-MICROSOFT-2022-NOVIEMBRE

**TLP: CLEAR**

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

## TABLA DE CONTENIDO

Sobre el BCSC ..... 3
1. Resumen ejecutivo ..... 4
2. Recursos afectados ..... 5
3. Análisis técnico ..... 7
4. Mitigación / Solución ..... 23
5. Referencias Adicionales ..... 24

## 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 noviembre de 2022. Con estas actualizaciones se corrigen 68 vulnerabilidades, siendo 10 de ellas calificadas como críticas, 56 como importantes y 2 sin un valor asignado. Hay que destacar que dentro de estas vulnerabilidades hay **5 zero-day**, **todas siendo explotadas y 1 divulgada públicamente.**

Estas vulnerabilidades afectan a productos como Windows Scripting, Microsoft Exchange Server, Windows Point-to-Point Tunneling, Windows Kerberos, Role: Windows Hyper-V, Windows CNG Key Isolation Service, entre otros.

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

- 4 vulnerabilidad de bypass.
- 6 vulnerabilidades de denegación de servicio.
- 9 vulnerabilidades de divulgación de información.
- 14 vulnerabilidades de ejecución remota de código.
- 25 vulnerabilidades de elevación de privilegios.
- 3 vulnerabilidades de spoofing.
- 1 vulnerabilidad de inyección de código.
- 2 vulnerabilidades de saturación del búfer.
- 1 vulnerabilidad en Github de optimización de repositorios clonados locales que deshacen la referencia a los enlaces simbólicos de forma predeterminada.
- 1 vulnerabilidad de suplantación de identidad.
- 2 vulnerabilidad de omisión de la característica de seguridad.

También se destaca en el informe la actualización con identificador ADV220003 para Microsoft Office como refuerzo en torno a los documentos protegidos por IRM para garantizar la cadena de certificados de confianza.

Se recomienda la aplicación de los parches para su corrección.

## 2. Recursos afectados

Las actualizaciones de seguridad del mes de noviembre de 2022 están asociadas a vulnerabilidades que afectan a los siguientes productos:

- .NET Framework
- AMD CPU Branch
- Azure
- Azure Real Time Operating System
- Linux Kernel
- Microsoft Dynamics
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Office Word
- Network Policy Server (NPS)
- Open Source Software
- Role: Windows Hyper-V
- SysInternals
- Visual Studio
- Windows Advanced Local Procedure Call
- Windows ALPC
- Windows Bind Filter Driver
- Windows BitLocker
- Windows CNG Key Isolation Service
- Windows Devices Human Interface
- Windows Digital Media
- Windows DWM Core Library
- Windows Extensible File Allocation
- Windows Group Policy Preference Client
- Windows HTTP.sys

- Windows Kerberos
- Windows Mark of the Web (MOTW)
- Windows Netlogon
- Windows Network Address Translation (NAT)
- Windows ODBC Driver
- Windows Overlay Filter
- Windows Point-to-Point Tunneling Protocol
- Windows Print Spooler Components
- Windows Resilient File System (ReFS)
- Windows Scripting
- Windows Win32K

## 3. Análisis técnico

A continuación, los detalles de las vulnerabilidades de más relevancia

corregidas en esta actualización son los siguientes:

Las cinco vulnerabilidades zero-day tratadas son:

CVE-2022-41128: vulnerabilidad de ejecución remota de código en lenguajes de secuencias de comandos de Windows. Esta vulnerabilidad requiere que un usuario con una versión afectada de Windows acceda a un servidor malicioso. Un atacante tendría que alojar un recurso compartido de servidor o un sitio web especialmente diseñado y convencer a las víctimas para que visitasen el sitio web o el servidor, generalmente a través técnicas de ingeniería social o campañas de phishing. **La vulnerabilidad está siendo explotada**.

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-2022-41073: vulnerabilidad de elevación de privilegios de la cola de impresión de Windows, de forma que un atacante que aprovechara con éxito esta vulnerabilidad podría obtener privilegios de sistema. **La vulnerabilidad está siendo explotada.**

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-2022-41125**:** vulnerabilidad de elevación de privilegios del servicio de aislamiento de claves CNG de Windows**,** de forma que un atacante que aprovechara con éxito esta vulnerabilidad podría obtener privilegios de sistema. **La vulnerabilidad está siendo explotada.**

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-2022-41091: vulnerabilidad de omisión de características de seguridad web de forma que un atacante puede crear un archivo malicioso que evadiría las defensas de Mark of the Web (MOTW), lo que daría como resultado una pérdida limitada de integridad y disponibilidad de funciones de seguridad como Vista protegida en Microsoft Office, que se basan en el etiquetado MOTW. **La vulnerabilidad está siendo explotada y ha sido divulgada públicamente.**

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

CVE-2022-3786: vulnerabilidad de desbordamiento del búfer de verificación de certificado X.509. **La vulnerabilidad está siendo explotada.**

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: Sin asignar

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

- **Vector de ataque**: **Red**

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

A continuación, todas las vulnerabilidades críticas tratadas que son las siguientes:

CVE-2022-41080: vulnerabilidad de elevación de privilegios de Microsoft Exchange Server.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.8

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

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

CVE-2022-41044: vulnerabilidad de ejecución remota de código del protocolo de tunelización punto a punto de Windows, de manera que, 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 la máquina del servidor RAS.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.1

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

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

CVE-2022-41088: vulnerabilidad de ejecución remota de código del protocolo de tunelización punto a punto de Windows. Para aprovechar esta vulnerabilidad, un atacante necesitaría enviar un paquete PPTP malicioso especialmente diseñado a un servidor PPTP, lo que podría resultar en la ejecución remota de código en el lado del servidor.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.1

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

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

CVE-2022-41039: vulnerabilidad de ejecución remota de código del protocolo de tunelización punto a punto de 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 la máquina del servidor RAS.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.1

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

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

CVE-2022-37966: vulnerabilidad de elevación de privilegios de Windows Kerberos RC4-HMAC. Destacar que la explotación exitosa de esta vulnerabilidad requiere que un atacante recopile información específica del entorno del componente objetivo y de tener éxito, podría obtener privilegios de administrador.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.1

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

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

CVE-2022-41118: vulnerabilidad de ejecución remota de código en lenguajes de secuencias de comandos de Windows. Esta vulnerabilidad requiere que un usuario con una versión afectada de Windows acceda a un servidor malicioso. Un atacante tendría que alojar un recurso compartido de servidor o un sitio web especialmente diseñado y convencer a las víctimas para que visitasen el sitio web o el servidor, generalmente a través técnicas de ingeniería social o campañas de phishing.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.5

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

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

CVE-2022-37967: vulnerabilidad de elevación de privilegios de Windows Kerberos de manera que un atacante autenticado podría aprovechar las vulnerabilidades del protocolo criptográfico en Windows Kerberos. Si el atacante obtiene el control del servicio que se permite para la delegación, puede modificar el PAC de Kerberos para elevar sus privilegios.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.2

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

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Altos
- **Interacción con el usuario**: **Ninguna**

- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-38015: vulnerabilidad de denegación de servicio de Windows Hyper-V de forma que la explotación exitosa de esta vulnerabilidad podría permitir que un invitado de Hyper-V afecte 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:N/UI:N/S:C/C:N/I:N/A:H

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

CVE-2022-39327: vulnerabilidad reportada por GitHub de control inadecuado de la generación de código, Inyección de código, en la CLI de Azure.

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**

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

| CVE | Descripción | Severidad | Divulgado | Explotado | CVSS |
|---|---|---|---|---|---|
| CVE-2022-41128 | Vulnerabilidad de ejecución remota de código en lenguajes de | Crítica | No | Sí | 8.8 |

| | | | | | |
|---|---|---|---|---|---|
| | scripting de Windows | | | | |
| CVE-2022-41080 | Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server | **Crítica** | No | No | 8.8 |
| CVE-2022-41044 | Vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a punto en Windows | **Crítica** | No | No | 8.1 |
| CVE-2022-41088 | Vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a punto en Windows | **Crítica** | No | No | 8.1 |
| CVE-2022-41039 | Vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a punto en Windows | **Crítica** | No | No | 8.1 |
| CVE-2022-37966 | Vulnerabilidad de elevación de privilegios en Windows Kerberos RC4-HMAC | **Crítica** | No | No | 8.1 |
| CVE-2022-41118 | Vulnerabilidad de ejecución remota de código en lenguajes de scripting de Windows | **Crítica** | No | No | 7.5 |
| CVE-2022-37967 | Vulnerabilidad de elevación de | **Crítica** | No | No | 7.2 |

| | | | | | |
|---|---|---|---|---|---|
| | privilegios Kerberos en Windows | | | | |
| CVE-2022-38015 | Vulnerabilidad de denegación de servicio en Windows Hyper-V | **Crítica** | No | No | 6.5 |
| CVE-2022-39327 | Control incorrecto de la generación de código (inyección de código) en la CLI de Azure | **Crítica** | No | No | Sin valor asigando por Microsoft, fallo reportado por GitHub |
| CVE-2022-41062 | Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server | Importante | No | No | 8.8 |
| CVE-2022-41047 | Vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft | Importante | No | No | 8.8 |
| CVE-2022-41048 | Vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft | Importante | No | No | 8.8 |
| CVE-2022-38023 | Vulnerabilidad de elevación de privilegios en Netlogon RPC | Importante | No | No | 8.1 |
| CVE-2022-41078 | Vulnerabilidad de suplantación de identidad en Microsoft Exchange Server | Importante | No | No | 8.0 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2022-41079 | Vulnerabilidad de suplantación de identidad en Microsoft Exchange Server | Importante | No | No | 8.0 |
| CVE-2022-41057 | Vulnerabilidad de elevación de privilegios en Windows HTTP.sys | Importante | No | No | 7.8 |
| CVE-2022-41054 | Vulnerabilidad de elevación de privilegios del Sistema de archivos resistente a Windows (ReFS) | Importante | No | No | 7.8 |
| CVE-2022-41096 | Vulnerabilidad de elevación de privilegios en la biblioteca principal de Microsoft DWM | Importante | No | No | 7.8 |
| CVE-2022-41106 | Vulnerabilidad de ejecución remota de código en Microsoft Excel | Importante | No | No | 7.8 |
| CVE-2022-41063 | Vulnerabilidad de ejecución remota de código en Microsoft Excel | Importante | No | No | 7.8 |
| CVE-2022-41107 | Vulnerabilidad de ejecución remota de código en Microsoft Office Graphics | Importante | No | No | 7.8 |
| CVE-2022-41109 | Vulnerabilidad de elevación de privilegios en Windows Win32k | Importante | No | No | 7.8 |
| CVE-2022-41113 | Vulnerabilidad de elevación de | Importante | No | No | 7.8 |

| | | | | | |
|---|---|---|---|---|---|
| | privilegios en el subsistema del kernel de Windows Win32 | | | | |
| CVE-2022-41073 | Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows | Importante | No | Sí | 7.8 |
| CVE-2022-41119 | Vulnerabilidad de ejecución remota de código en Visual Studio | Importante | No | No | 7.8 |
| CVE-2022-41061 | Vulnerabilidad de ejecución remota de código en Microsoft Word | Importante | No | No | 7.8 |
| CVE-2022-41095 | Vulnerabilidad de elevación de privilegios en el receptor de medios digitales de Windows | Importante | No | No | 7.8 |
| CVE-2022-41051 | Vulnerabilidad de ejecución remota de código en Azure RTOS GUIX Studio | Importante | No | No | 7.8 |
| CVE-2022-41100 | Vulnerabilidad de elevación de privilegios en Windows Advanced Local Procedure Call (ALPC) | Importante | No | No | 7.8 |
| CVE-2022-41101 | Vulnerabilidad de elevación de privilegios en el filtro de superposición de Windows | Importante | No | No | 7.8 |
| CVE-2022-41102 | Vulnerabilidad de elevación de | Importante | No | No | 7.8 |

| | | | | | |
|---|---|---|---|---|---|
| | privilegios en el filtro de superposición de Windows | | | | |
| CVE-2022-41120 | Vulnerabilidad de elevación de privilegios en Sysmon en Microsoft Windows | Importante | No | No | 7.8 |
| CVE-2022-41123 | Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server | Importante | No | No | 7.8 |
| CVE-2022-41052 | Vulnerabilidad de ejecución remota de código en el componente de gráficos de Windows | Importante | No | No | 7.8 |
| CVE-2022-41045 | Vulnerabilidad de elevación de privilegios en Windows Advanced Local Procedure Call (ALPC) | Importante | No | No | 7.8 |
| CVE-2022-41093 | Vulnerabilidad de elevación de privilegios en Windows Advanced Local Procedure Call (ALPC) | Importante | No | No | 7.8 |
| CVE-2022-41050 | Vulnerabilidad de elevación de privilegios en la tabla de asignación extensible de archivos de Windows | Importante | No | No | 7.8 |
| CVE-2022-37992 | Vulnerabilidad de elevación de | Importante | No | No | 7.8 |

| | | | | | |
|---|---|---|---|---|---|
| | privilegios en la directiva de grupo de Windows | | | | |
| CVE-2022-41092 | Vulnerabilidad de elevación de privilegios en Windows Win32k | Importante | No | No | 7.8 |
| CVE-2022-41125 | Vulnerabilidad de elevación de privilegios en el servicio de aislamiento en Windows CNG Key | Importante | No | Sí | 7.8 |
| CVE-2022-41056 | Vulnerabilidad de denegación de servicio en el protocolo RADIUS del servidor de directivas de redes (NPS) | Importante | No | No | 7.5 |
| CVE-2022-41053 | Vulnerabilidad de denegación de servicio en Kerberos en Windows | Importante | No | No | 7.5 |
| CVE-2022-41058 | Vulnerabilidad de denegación de servicio en la traducción de direcciones de red (NAT) de Windows | Importante | No | No | 7.5 |
| CVE-2022-41085 | Vulnerabilidad de elevación de privilegios en Azure CycleCloud | Importante | No | No | 7.5 |
| CVE-2022-41114 | Vulnerabilidad de elevación de privilegios en el controlador de filtro de enlace de Windows | Importante | No | No | 7.0 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2022-38014 | Vulnerabilidad de elevación de privilegios en el kernel del subsistema de Windows para Linux (WSL2) | Importante | No | No | 7.0 |
| CVE-2022-41097 | Vulnerabilidad de divulgación de información del protocolo RADIUS del servidor de directivas de redes (NPS) | Importante | No | No | 6.5 |
| CVE-2022-41122 | Vulnerabilidad de suplantación de identidad en Microsoft SharePoint Server | Importante | No | No | 6.5 |
| CVE-2022-41086 | Vulnerabilidad de elevación de privilegios en la directiva de grupo de Windows | Importante | No | No | 6.4 |
| CVE-2022-41090 | Vulnerabilidad de denegación de servicio del protocolo de túnel punto a punto en Windows | Importante | No | No | 5.9 |
| CVE-2022-41116 | Vulnerabilidad de denegación de servicio del protocolo de túnel punto a punto en Windows | Importante | No | No | 5.9 |
| CVE-2022-41064 | Vulnerabilidad de divulgación de información en .NET Framework | Importante | No | No | 5.8 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2022-41055 | Vulnerabilidad de divulgación de información de dispositivos de interfaz humana en Windows | Importante | No | No | 5.5 |
| CVE-2022-41060 | Vulnerabilidad de divulgación de información en Microsoft Word | Importante | No | No | 5.5 |
| CVE-2022-41103 | Vulnerabilidad de divulgación de información en Microsoft Word | Importante | No | No | 5.5 |
| CVE-2022-41098 | Vulnerabilidad de divulgación de información en GDI+ en Windows | Importante | No | No | 5.5 |
| CVE-2022-41104 | Vulnerabilidad de omisión de característica de seguridad en Microsoft Excel | Importante | No | No | 5.5 |
| CVE-2022-41105 | Vulnerabilidad de divulgación de información en Microsoft Excel | Importante | No | No | 5.5 |
| CVE-2022-41049 | Marca en Windows de la vulnerabilidad de omisión de característica de seguridad web | Importante | No | No | 5.4 |
| CVE-2022-41091 | Marca en Windows de la vulnerabilidad de omisión de característica de seguridad web | Importante | Sí | Sí | 5.4 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2022-41099 | Vulnerabilidad de omisión de la característica de seguridad de BitLocker | Importante | No | No | 4.6 |
| CVE-2022-41066 | Vulnerabilidad de divulgación de información en Microsoft Business Central | Importante | No | No | 4.4 |
| CVE-2022-23824 | IBPB e interacciones predictoras de direcciones de retorno, potencial divulgación de información | Importante | No | No | Sin valor asignado por Microsoft, el fallo es tratado por AMD |
| ADV220003 | Actualización en profundidad de Microsoft Defense | Importante | No | No | Sin valor asignado |
| CVE-2022-39253 | La optimización de clones locales (repositorios) deshace la referencia a los enlaces simbólicos de forma predeterminada | Importante | No | No | Sin valor asignado por Microsoft, fallo reportado por GitHub |
| CVE-2022-3602 | Desbordamiento del búfer de verificación de certificados X.509 | Sin valor asignado | No | No | Sin valor asignado por Microsoft, fallo reportado por OpenSSL Software Foundation |
| CVE-2022-3786 | Desbordamiento del búfer de verificación de | Sin valor asignado | No | Sí | Sin valor asignado por Microsoft, |

| | | | | | |
|---|---|---|---|---|---|
| | certificados X.509 | | | | fallo reportado por OpenSSL Software Foundation |

## 4. Mitigación / Solución

Para la mitigación y el parcheo 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

- November 2022 Security Updates
- Security Update Guide - Microsoft
- Zero Day initiative-The November 2022 Security Update Review


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA