Basque CyberSecurity Centre

Actualización de seguridad de Microsoft-Octubre 2022

BCSC-ACTUALIZACIONES-MICROSOFT-2022-OCTUBRE

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 octubre de 2022. Con estas actualizaciones se corrigen 84 vulnerabilidades, siendo 13 de ellas calificadas como críticas, 69 como importantes, 1 moderada y 1 sin un valor asignado. A estas vulnerabilidades hay que añadir otras 11 corregidas en el navegador Edge basado en Chromium, para las que Microsoft no ha establecido un nivel de severidad. Estas vulnerabilidades afectan a productos como Azure, Azure Arc, Windows COM+ Event System Service, Windows Kernel, Microsoft Office, Microsoft Office SharePoint y Microsoft Office Word, entre otros.

Cabe destacar que las recientes vulnerabilidades zero-day reportadas en Microsoft Exchange, no han sido tratadas en estas actualizaciones.

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

- 2 vulnerabilidad de bypass.
- 8 vulnerabilidades de denegación de servicio.
- 11 vulnerabilidades de divulgación de información.
- 20 vulnerabilidades de ejecución remota de código.
- 39 vulnerabilidades de elevación de privilegios.
- 4 vulnerabilidades de spoofing.

Se recomienda la aplicación de los parches para su corrección.

2. Recursos afectados

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

- Active Directory Domain Services
- Azure
- Azure Arc
- Client Server Run-time Subsystem (CSRSS)
- Microsoft Edge (basado en Chromium)
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Office Word
- Microsoft WDAC OLE DB provider for SQL
- NuGet Client
- Remote Access Service Point-to-Point Tunneling Protocol
- Role: Windows Hyper-V
- Service Fabric
- Visual Studio Code
- Windows Active Directory Certificate Services
- Windows ALPC
- Windows CD-ROM Driver
- Windows COM+ Event System Service
- Windows Connected User Experiences and Telemetry
- Windows CryptoAPI
- Windows Defender
- Windows DHCP Client
- Windows Distributed File System (DFS)
- Windows DWM Core Library
- Windows Event Logging Service
- Windows Group Policy
- Windows Group Policy Preference Client

- Windows Internet Key Exchange (IKE) Protocol
- Windows Kernel
- Windows Local Security Authority (LSA)
- Windows Local Security Authority Subsystem Service (LSASS)
- Windows Local Session Manager (LSM)
- Windows NTFS
- Windows NTLM
- Windows ODBC Driver
- Windows Perception Simulation Service
- Windows Point-to-Point Tunneling Protocol
- Windows Portable Device Enumerator Service
- Windows Print Spooler Components
- Windows Resilient File System (ReFS)
- Windows Secure Channel
- Windows Security Support Provider Interface
- Windows Server Remotely Accessible Registry Keys
- Windows Server Service
- Windows Storage
- Windows TCP/IP
- Windows USB Serial Driver
- Windows Web Account Manager
- Windows Win32K
- Windows WLAN Service
- Windows Workstation Service

3. Análisis técnico

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

Las dos vulnerabilidades zero-day tratadas son:

CVE-2022-41033: vulnerabilidad de elevación de privilegios del servicio del sistema de eventos COM+ de Windows, **que está siendo explotada,** aunque no ha sido divulgada.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.8

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-2022-41043: vulnerabilidad de divulgación de información de Microsoft Office que **ha sido divulgada,** aunque no explotada.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 3.3
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

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

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

CVE-2022-37968: vulnerabilidad de elevación de privilegios en el clúster de Kubernetes habilitado para Azure Arc. Esta vulnerabilidad podría permitir que un usuario no autenticado eleve sus privilegios y potencialmente obtenga control

administrativo sobre el clúster de Kubernetes. Además, dado que Azure Stack Edge permite a los usuarios del mismo implementar cargas de trabajo de Kubernetes en sus dispositivos a través de Azure Arc, los dispositivos de Azure Stack Edge también son vulnerables a esta vulnerabilidad.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 10.0

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

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

CVE-2022-37976: vulnerabilidad de elevación de privilegios de servicios de certificados de Active Directory, de forma que un cliente DCOM malicioso puede obligar a un servidor DCOM a autenticarse a través del Servicio de certificados de Active Directory (ADCS) y usar la credencial para lanzar un ataque entre protocolos, permitiendo al atacante obtener privilegios de administrador de dominio.

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-2022-41038: vulnerabilidad de ejecución remota de código de Microsoft SharePoint Server con lo que, en un hipotético ataque en red, un atacante autenticado con permisos de administrar listas podría ejecutar código de forma remota en el servidor de SharePoint.

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-2022-30198: vulnerabilidad de ejecución remota de código del protocolo de tunelización punto a punto de Windows, de forma que, 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-2022-22035: vulnerabilidad de ejecución remota de código del protocolo de tunelización punto a punto de Windows, de modo que, para poder explotar esta vulnerabilidad, un atacante necesitaría enviar un paquete PPTP malicioso especialmente diseñado a un servidor PPTP. Esto 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-2022-24504: vulnerabilidad de ejecución remota de código del protocolo de tunelización punto a punto de Windows, de forma que, 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-2022-33634: vulnerabilidad de ejecución remota de código del protocolo de tunelización punto a punto de Windows, de modo que, para poder explotar esta vulnerabilidad, un atacante necesitaría enviar un paquete PPTP malicioso especialmente diseñado a un servidor PPTP. Esto 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-2022-38047: vulnerabilidad de ejecución remota de código del protocolo de tunelización punto a punto de Windows, de forma que, 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-2022-38000: vulnerabilidad de ejecución remota de código del protocolo de tunelización punto a punto de Windows, de forma que, 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-2022-41081: vulnerabilidad de ejecución remota de código del protocolo de tunelización punto a punto de Windows, de forma que, 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-2022-38048: vulnerabilidad de ejecución remota de código de Microsoft Office.

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-2022-37979: vulnerabilidad de elevación de privilegios de Windows Hyper-V, de modo que un atacante en un entorno de Hyper-V anidado obtendría privilegios de sistema operativo raíz de Windows en Hyper-V de nivel 1, lo que implicaría 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: 7.8

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

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

CVE-2022-34689: vulnerabilidad de falsificación de CryptoAPI de Windows, de manera que un atacante podría manipular un certificado x.509 público existente para falsificar su identidad y realizar acciones como autenticación o firma de código como el certificado de destino.

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:N/I:H/A:N

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

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

CVE	Descripción	Severidad	Divulgado	Explotado	CVSS
CVE-2022-37968	Vulnerabilidad de elevación de privilegios en el clúster de Kubernetes habilitado para Azure Arc Connect	**Crítica**	No	No	10.0
CVE-2022-37976	Vulnerabilidad de elevación de privilegios en servicios de certificados de Active Directory	**Crítica**	No	No	8.8
CVE-2022-41038	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	**Crítica**	No	No	8.8
CVE-2022-30198	Vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a punto de Windows	**Crítica**	No	No	8.1
CVE-2022-22035	Vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a	**Crítica**	No	No	8.1

	punto de Windows				
CVE-2022-24504	Vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a punto de Windows	**Crítica**	No	No	8.1
CVE-2022-33634	Vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a punto de Windows	**Crítica**	No	No	8.1
CVE-2022-38047	Vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a punto de Windows	**Crítica**	No	No	8.1
CVE-2022-38000	Vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a punto de Windows	**Crítica**	No	No	8.1
CVE-2022-41081	Vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a punto de Windows	**Crítica**	No	No	8.1
CVE-2022-38048	Vulnerabilidad de ejecución remota de código en Microsoft Office	**Crítica**	No	No	7.8

CVE-2022-37979	Vulnerabilidad de elevación de privilegios en Windows Hyper-V	**Crítica**	No	No	7.8
CVE-2022-34689	Vulnerabilidad de spoofing de cryptoAPI en Windows	**Crítica**	No	No	7.5
CVE-2022-41036	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	Importante	No	No	8.8
CVE-2022-41037	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	Importante	No	No	8.8
CVE-2022-38016	Vulnerabilidad de elevación de privilegios en la Autoridad de seguridad local (LSA) de Windows	Importante	No	No	8.8
CVE-2022-37982	Vulnerabilidad de ejecución remota de código en el proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8
CVE-2022-38031	Vulnerabilidad de ejecución remota de código en el proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8

CVE-2022-38040	Vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft	Importante	No	No	8.8
CVE-2022-38045	Vulnerabilidad de elevación de privilegios en el protocolo remoto del servicio de servidor	Importante	No	No	8.8
CVE-2022-38053	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	Importante	No	No	8.8
CVE-2022-33635	Vulnerabilidad de ejecución remota de código en Windows GDI+	Importante	No	No	7.8
CVE-2022-37970	Vulnerabilidad de elevación de privilegios en la biblioteca principal de DWM de Windows	Importante	No	No	7.8
CVE-2022-37986	Vulnerabilidad de elevación de privilegios en Windows Win32k	Importante	No	No	7.8
CVE-2022-37987	Vulnerabilidad de elevación de privilegios en el subsistema en tiempo de ejecución de Windows Client Server (CSRSS)	Importante	No	No	7.8

CVE-2022-37999	Vulnerabilidad de elevación de privilegios en el cliente de preferencias de directiva de grupo de Windows	Importante	No	No	7.8
CVE-2022-38049	Vulnerabilidad de ejecución remota de código en Microsoft Office Graphics	Importante	No	No	7.8
CVE-2022-38050	Vulnerabilidad de elevación de privilegios en Win32k	Importante	No	No	7.8
CVE-2022-38051	Vulnerabilidad de elevación de privilegios en el componente de gráficos de Windows	Importante	No	No	7.8
CVE-2022-38003	Elevación de privilegios del sistema de archivos resistente de Windows	Importante	No	No	7.8
CVE-2022-41032	Vulnerabilidad de elevación de privilegios en el cliente NuGet	Importante	No	No	7.8
CVE-2022-41034	Vulnerabilidad de ejecución remota de código en Visual Studio Code	Importante	No	No	7.8
CVE-2022-37975	Vulnerabilidad de elevación de privilegios en la directiva de grupo de Windows	Importante	No	No	7.8

CVE-2022-38028	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	No	No	7.8
CVE-2022-37980	Vulnerabilidad de elevación de privilegios en el cliente DHCP de Windows	Importante	No	No	7.8
CVE-2022-37983	Vulnerabilidad de elevación de privilegios en la biblioteca principal de DwM de Microsoft	Importante	No	No	7.8
CVE-2022-37984	Vulnerabilidad de elevación de privilegios en el servicio WLAN de Windows	Importante	No	No	7.8
CVE-2022-37988	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2022-38037	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2022-37989	Vulnerabilidad de elevación de privilegios en el subsistema en tiempo de ejecución de Windows Client Server (CSRSS)	Importante	No	No	7.8
CVE-2022-38038	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8

CVE-2022-37990	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2022-38039	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2022-37991	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2022-37993	Vulnerabilidad de elevación de privilegios en el cliente de preferencias de directiva de grupo de Windows	Importante	No	No	7.8
CVE-2022-37994	Vulnerabilidad de elevación de privilegios en el cliente de preferencias de directiva de grupo de Windows	Importante	No	No	7.8
CVE-2022-37995	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2022-37997	Vulnerabilidad de elevación de privilegios en el componente de gráficos de Windows	Importante	No	No	7.8
CVE-2022-41031	Vulnerabilidad de ejecución remota de código en Microsoft Word	Importante	No	No	7.8

CVE-2022-41033	Vulnerabilidad de elevación de privilegios en el servicio del sistema de eventos WINDOWS COM+	Importante	No	Sí	7.8
CVE-2022-41083	Vulnerabilidad de elevación de privilegios en Visual Studio Code	Importante	No	No	7.8
CVE-2022-37998	Vulnerabilidad de denegación de servicio en el Administrador de sesiones locales de Windows (LSM)	Importante	No	No	7.7
CVE-2022-37973	Vulnerabilidad de denegación de servicio en el Administrador de sesiones locales de Windows (LSM)	Importante	No	No	7.7
CVE-2022-33645	Vulnerabilidad de denegación de servicio en el controlador TCP/IP de Windows	Importante	No	No	7.5
CVE-2022-38036	Vulnerabilidad de denegación de servicio en el protocolo de intercambio de claves de Internet (IKE)	Importante	No	No	7.5
CVE-2022-37978	Omisión de la característica de seguridad de Servicios de certificados de Windows Active Directory	Importante	No	No	7.5

CVE-2022-38041	Vulnerabilidad de denegación de servicio en el canal seguro de Windows	Importante	No	No	7.5
CVE-2022-41042	Vulnerabilidad de divulgación de información en Visual Studio Code	Importante	No	No	7.4
CVE-2022-37971	Vulnerabilidad de elevación de privilegios en Microsoft Windows Defender	Importante	No	No	7.1
CVE-2022-38042	Vulnerabilidad de elevación de privilegios en los Servicios de dominio de Active Directory	Importante	No	No	7.1
CVE-2022-38021	Vulnerabilidad de elevación de privilegios en Experiencias de usuario conectadas y telemetría	Importante	No	No	7.0
CVE-2022-38027	Vulnerabilidad de elevación de privilegios en el almacenamiento de Windows	Importante	No	No	7.0
CVE-2022-38029	Vulnerabilidad de elevación de privilegios en Windows ALPC	Importante	No	No	7.0
CVE-2022-38017	Vulnerabilidad de elevación de privilegios en StorSimple serie 8000	Importante	No	No	6.8
CVE-2022-35770	Vulnerabilidad de suplantación de identidad de Windows NTLM	Importante	No	No	6.5

CVE-2022-38001	Vulnerabilidad de suplantación de identidad en Microsoft Office	Importante	No	No	6.5
CVE-2022-37974	Vulnerabilidad de divulgación de información en Windows Mixed Reality Developer Tools	Importante	No	No	6.5
CVE-2022-37977	Vulnerabilidad de denegación de servicio del servicio de subsistema de autoridad de seguridad local (LSASS)	Importante	No	No	6.5
CVE-2022-38033	Vulnerabilidad de divulgación de información de claves del Registro de acceso remoto en Windows Server	Importante	No	No	6.5
CVE-2022-35829	Vulnerabilidad de spoofing en el Explorador de Service Fabric	Importante	No	No	6.2
CVE-2022-38046	Vulnerabilidad de divulgación de información en Web Account Manager	Importante	No	No	6.2
CVE-2022-37965	Vulnerabilidad de denegación de servicio en el protocolo de túnel punto a punto de Windows	Importante	No	No	5.9
CVE-2022-38032	Vulnerabilidad de omisión de la característica de seguridad del servicio	Importante	No	No	5.9

	enumerador de dispositivos portátiles de Windows				
CVE-2022-38025	Vulnerabilidad de divulgación de información en el sistema de archivos distribuido (DFS) de Windows	Importante	No	No	5.5
CVE-2022-38026	Vulnerabilidad de divulgación de información de cliente DHCP en Windows	Importante	No	No	5.5
CVE-2022-37985	Vulnerabilidad de divulgación de información de componentes de gráficos de Windows	Importante	No	No	5.5
CVE-2022-38043	Vulnerabilidad de divulgación de información en la interfaz del proveedor de soporte técnico de seguridad de Windows	Importante	No	No	5.5
CVE-2022-37996	Vulnerabilidad de divulgación de información de memoria en el kernel de Windows	Importante	No	No	5.5
CVE-2022-38034	Vulnerabilidad de elevación de privilegios en el servicio windows workstation	Importante	No	No	4.3
CVE-2022-37981	Vulnerabilidad de denegación de servicio en el servicio de	Importante	No	No	4.3

	registro de eventos de Windows				
CVE-2022-38030	Vulnerabilidad de divulgación de información del controlador serie USB de Windows	Importante	No	No	4.3
CVE-2022-41043	Vulnerabilidad de divulgación de información en Microsoft Office	Importante	Sí	No	3.3
CVE-2022-38022	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	2.5
CVE-2022-41035	Microsoft Edge (basado en Chromium) vulnerabilidad de Spoofing	Moderada	No	No	8.3
CVE-2022-38044	Vulnerabilidad de ejecución remota de código en el controlador del sistema de archivos de CD-ROM de Windows	Sin valor asignado	No	No	7.8
CVE-2022-3304	Chromium: Uso después de la liberación en CSS	Sin valor asignado	No	No	6.2
CVE-2022-3307	Chromium: Uso después de la gratuidad en los medios	Sin valor asignado	No	No	6.2
CVE-2022-3308	Chromium: Aplicación insuficiente de directivas en las herramientas de desarrollo	Sin valor asignado	No	No	6.2

CVE-2022-3310	Chromium: Aplicación de directivas insuficiente en fichas personalizadas	Sin valor asignado	No	No	6.2
CVE-2022-3311	Chromium: Uso después de liberar en Importación	Sin valor asignado	No	No	6.2
CVE-2022-3313	Chromium: Interfaz de usuario de seguridad incorrecta en pantalla completa	Sin valor asignado	No	No	6.2
CVE-2022-3315	Chromium: Confusión en Blink	Sin valor asignado	No	No	6.2
CVE-2022-3316	Chromium: Validación insuficiente de la entrada que no es de confianza en la navegación segura	Sin valor asignado	No	No	6.2
CVE-2022-3317	Chromium: Validación insuficiente de entradas que no son de confianza en Intents	Sin valor asignado	No	No	6.2
CVE-2022-3370	Chromium: Uso después de la liberación en Elementos personalizados	Sin valor asignado	No	No	6.2
CVE-2022-3373	Chromium: Escritura fuera de los límites en V8	Sin valor asignado	No	No	6.2

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

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

Basque CyberSecurity Centre

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA