Basque CyberSecurity Centre

Actualización de seguridad de Microsoft-Agosto 2022

BCSC-ACTUALIZACIONES-MICROSOFT-2022-AGOSTO

TLP:WHITE

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 agosto de 2022. Con estas actualizaciones se corrigen 125 vulnerabilidades, siendo 17 de ellas calificadas como críticas, 106 como importantes, 1 moderada y 1 baja. A estas vulnerabilidades hay que añadir otras 17 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 .NET Core, Active Directory Domain Services, Microsoft Office, Microsoft Office Excel, Microsoft Office Outlook, Microsoft Windows Support Diagnostic Tool (MSDT) y Windows Network File System entre otros.

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

- 7 vulnerabilidades de bypass.
- 7 vulnerabilidades de denegación de servicio
- 12 vulnerabilidades de divulgación de información.
- 32 vulnerabilidades de ejecución remota de código.
- 66 vulnerabilidades de elevación de privilegios.
- 1 vulnerabilidad de spoofing.

Se recomienda la aplicación de los parches para su corrección.

2. Recursos afectados

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

- .NET Core
- Active Directory Domain Services
- Azure Batch Node Agent
- Azure Real Time Operating System
- Azure Site Recovery
- Azure Sphere
- Microsoft ATA Port Driver
- Microsoft Bluetooth Driver
- Microsoft Edge (Chromium-based)
- Microsoft Exchange Server
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office Outlook
- Microsoft Windows Support Diagnostic Tool (MSDT)
- Remote Access Service Point-to-Point Tunneling Protocol
- Role: Windows Fax Service
- Role: Windows Hyper-V
- System Center Operations Manager
- Visual Studio
- Windows Bluetooth Service
- Windows Canonical Display Driver
- Windows Cloud Files Mini Filter Driver
- Windows Defender Credential Guard
- Windows Digital Media
- Windows Error Reporting
- Windows Hello
- Windows Internet Information Services
- Windows Kerberos
- Windows Kernel

- Windows Local Security Authority (LSA)
- Windows Network File System
- Windows Partition Management Driver
- Windows Point-to-Point Tunneling Protocol
- Windows Print Spooler Components
- Windows Secure Boot
- Windows Secure Socket Tunneling Protocol (SSTP)
- Windows Storage Spaces Direct
- Windows Unified Write Filter
- Windows WebBrowser Control
- Windows Win32K

3. Análisis técnico

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

CVE-2022-34713: vulnerabilidad de ejecución remota de código que afecta a Microsoft Windows Support Diagnostic Tool (MSDT), **que ha sido divulgada y está siendo explotada activamente.**

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-2022-30134: vulnerabilidad de divulgación de información que afecta a Microsoft Exchange de forma que un atacante que explotara con éxito la vulnerabilidad podría leer mensajes de correo electrónico de la víctima. Este fallo **ha sido divulgado públicamente**.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.6

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

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

Los detalles de las vulnerabilidades críticas corregidas en esta actualización son**:**

CVE-2022-30133: vulnerabilidad de ejecución remota de código en el protocolo Point To Point (PPP). Sólo se puede explotar mediante la comunicación a través del puerto 1723. Microsoft ofrece como solución temporal antes de instalar las

actualizaciones que abordan esta vulnerabilidad, bloquear el tráfico a través de ese puerto, lo que hace que la vulnerabilidad no se pueda explotar.

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

CVE-2022-35744: vulnerabilidad de ejecución remota de código en el protocolo Point To Point (PPP). Sólo se puede explotar mediante la comunicación a través del puerto 1723. Microsoft ofrece como solución temporal antes de instalar las actualizaciones que abordan esta vulnerabilidad, bloquear el tráfico a través de ese puerto, lo que hace que la vulnerabilidad no se pueda explotar.

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

CVE-2022-34691: vulnerabilidad de elevación de privilegios en Active Directory Domain Services. La mitigación ofrecida por Microsoft se refiere a una configuración, configuración común o mejor práctica general, existente en un estado predeterminado, que podría reducir la gravedad de la explotación de esta vulnerabilidad. Un sistema es vulnerable a este fallo solo si los servicios de certificados de Active Directory se ejecutan en el 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**: a nivel de **red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Bajos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-35804: vulnerabilidad de ejecución remota de código en SMB Client and Server, de forma que el protocolo Microsoft Server Message Block 3.1.1 (SMBv3) maneja ciertas solicitudes y un atacante que explotara con éxito 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: 8.8

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

- **Vector de ataque**: a nivel de **red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Requeridos
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-34714: vulnerabilidad de ejecución remota de código en el Windows Secure Socket Tunneling Protocol (SSTP), de forma que un atacante no autenticado podría enviar una solicitud de conexión especialmente diseñada a un servidor RAS, lo que podría conducir a 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**: a nivel de **red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Ninguno
- **Alcance**: Sin cambios

- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-35745: vulnerabilidad de ejecución remota de código en el Windows Secure Socket Tunneling Protocol (SSTP), de forma que un atacante no autenticado podría enviar una solicitud de conexión especialmente diseñada a un servidor RAS, lo que podría conducir a 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**: a nivel de **red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Ninguno
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-35752: vulnerabilidad de ejecución remota de código en el Windows Secure Socket Tunneling Protocol (SSTP) de forma que el sistema vulnerable puede ser explotado sin ninguna interacción por parte de ningún usuario.

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**: a nivel de **red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Ninguno
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-35753: vulnerabilidad de ejecución remota de código en el Windows Secure Socket Tunneling Protocol (SSTP) de forma que el sistema vulnerable puede ser explotado sin ninguna interacción por parte de ningún usuario.

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**: a nivel de **red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Ninguno
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-34702: vulnerabilidad de ejecución remota de código en el Windows Secure Socket Tunneling Protocol (SSTP) de forma 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**: a nivel de **red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Ninguno
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-35766: vulnerabilidad de ejecución remota de código en el Windows Secure Socket Tunneling Protocol (SSTP) de forma 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**: a nivel de **red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ningunos**

- **Interacción con el usuario**: Ninguno
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-35767: vulnerabilidad de ejecución remota de código en el Windows Secure Socket Tunneling Protocol (SSTP) de forma 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**: a nivel de **red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Ninguno
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-35794: vulnerabilidad de ejecución remota de código en el Windows Secure Socket Tunneling Protocol (SSTP) de forma 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**: a nivel de **red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Ninguno
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-21980: vulnerabilidad de elevación de privilegios en Microsoft Exchange Server. Esta vulnerabilidad requiere que un usuario con una versión afectada de Exchange Server acceda a un servidor malicioso. Un atacante tendría que alojar un recurso compartido de servidor o un sitio web especialmente diseñado y tendría que convencerlos usando técnicas de ingeniería social para que visiten el recurso compartido de servidor o sitio web, generalmente a través de en un mensaje de correo electrónico.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.1

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

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

CVE-2022-24516: vulnerabilidad de elevación de privilegios de Microsoft Exchange Server.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.0

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

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

CVE-2022-24477: vulnerabilidad de elevación de privilegios de Microsoft Exchange Server. Un atacante podría apoderarse de los buzones de correo de todos los usuarios de Exchange, pudiendo enviar correos electrónicos, leer correos electrónicos y descargar archivos adjuntos.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.0

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

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

CVE-2022-34696: Vulnerabilidad de ejecución remota de código de Windows Hyper-V. Un atacante autenticado que aproveche con éxito una condición de invitado de Hyper-V podría intentar activar un código malicioso en el contexto de ese usuario para intentar una ejecución de código arbitraria o remota en el 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**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-33646: Vulnerabilidad de elevación de privilegios del agente de nodo de Azure Batch. La explotación exitosa de esta vulnerabilidad requiere que un atacante prepare el entorno de la víctima para mejorar las posibilidades de la explotación.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.0

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

- **Vector de ataque**: local
- **Complejidad del ataque**: Alta
- **Privilegios requeridos:** Bajos
- **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-2022-30133	Vulnerabilidad de ejecución remota de código en el Protocolo punto a punto (PPP) de Windows	**Crítica**	No	No	9.8
CVE-2022-35744	Vulnerabilidad de ejecución remota de código en el Protocolo punto a punto (PPP) de Windows	**Crítica**	No	No	9.8
CVE-2022-34691	Vulnerabilidad de elevación de privilegios en los Servicios de dominio de Active Directory	**Crítica**	No	No	8.8
CVE-2022-35804	Vulnerabilidad de ejecución remota de código en el cliente y servidor SMB	**Crítica**	No	No	8.8
CVE-2022-34714	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets seguros (SSTP) de Windows	**Crítica**	No	No	8.1
CVE-2022-35745	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets seguros (SSTP) de Windows	**Crítica**	No	No	8.1
CVE-2022-35752	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets	**Crítica**	No	No	8.1

	seguros (SSTP) de Windows				
CVE-2022-35753	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets seguros (SSTP) de Windows	**Crítica**	No	No	8.1
CVE-2022-34702	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets seguros (SSTP) de Windows	**Crítica**	No	No	8.1
CVE-2022-35766	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets seguros (SSTP) de Windows	**Crítica**	No	No	8.1
CVE-2022-35767	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets seguros (SSTP) de Windows	**Crítica**	No	No	8.1
CVE-2022-35794	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets seguros (SSTP) de Windows	**Crítica**	No	No	8.1
CVE-2022-21980	Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server	**Crítica**	No	No	8.0
CVE-2022-24516	Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server	**Crítica**	No	No	8.0

CVE-2022-24477	Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server	**Crítica**	No	No	8.0
CVE-2022-34696	Vulnerabilidad de ejecución remota de código en Windows Hyper-V	**Crítica**	No	No	7.8
CVE-2022-33646	Vulnerabilidad de elevación de privilegios en azure Batch Node Agent	**Crítica**	No	No	7.0
CVE-2022-34715	Vulnerabilidad de ejecución remota de código en el sistema de archivos de red de Windows	Importante	No	No	9.8
CVE-2022-33649	Vulnerabilidad de omisión de la característica de seguridad de Microsoft Edge (basada en Chromium)	Importante	No	No	9.6
CVE-2022-34717	Vulnerabilidad de ejecución remota de código en Microsoft Office	Importante	No	No	8.8
CVE-2022-35777	Vulnerabilidad de ejecución remota de código en Visual Studio	Importante	No	No	8.8
CVE-2022-35825	Vulnerabilidad de ejecución remota de código en Visual Studio	Importante	No	No	8.8
CVE-2022-35826	Vulnerabilidad de ejecución remota de código en Visual Studio	Importante	No	No	8.8
CVE-2022-35827	Vulnerabilidad de ejecución remota de código en Visual Studio	Importante	No	No	8.8

CVE-2022-35761	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	8.4
CVE-2022-35802	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	8.1
CVE-2022-30175	Vulnerabilidad de ejecución remota de código en Azure RTOS GUIX Studio	Importante	No	No	7.8
CVE-2022-30176	Vulnerabilidad de ejecución remota de código en Azure RTOS GUIX Studio	Importante	No	No	7.8
CVE-2022-33640	System Center Operations Manager: Vulnerabilidad de elevación de privilegios en la infraestructura de administración abierta (OMI)	Importante	No	No	7.8
CVE-2022-33648	Vulnerabilidad de ejecución remota de código en Microsoft Excel	Importante	No	No	7.8
CVE-2022-33670	Vulnerabilidad de elevación de privilegios en el controlador de administración de particiones de Windows	Importante	No	No	7.8
CVE-2022-34687	Vulnerabilidad de ejecución remota de código en Azure RTOS GUIX Studio	Importante	No	No	7.8
CVE-2022-34699	Vulnerabilidad de elevación de	Importante	No	No	7.8

	privilegios en Windows Win32k				
CVE-2022-34703	Vulnerabilidad de elevación de privilegios en el controlador de administración de particiones de Windows	Importante	No	No	7.8
CVE-2022-34706	Vulnerabilidad de elevación de privilegios en la Autoridad de seguridad local (LSA) de Windows	Importante	No	No	7.8
CVE-2022-34707	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2022-34713	Vulnerabilidad de ejecución remota de código en la Herramienta de diagnóstico de soporte técnico de Microsoft Windows (MSDT)	Importante	Sí	Sí	7.8
CVE-2022-35743	Vulnerabilidad de ejecución remota de código en la Herramienta de diagnóstico de soporte técnico de Microsoft Windows (MSDT)	Importante	No	No	7.8
CVE-2022-35746	Vulnerabilidad de elevación de privilegios en Windows Digital Media Receiver	Importante	No	No	7.8
CVE-2022-35749	Vulnerabilidad de elevación de privilegios en Windows Digital Media Receiver	Importante	No	No	7.8

CVE-2022-35750	Vulnerabilidad de elevación de privilegios en Win32k	Importante	No	No	7.8
CVE-2022-35751	Vulnerabilidad de elevación de privilegios en Windows Hyper-V	Importante	No	No	7.8
CVE-2022-35756	Vulnerabilidad de elevación de privilegios en Kerberos de Windows	Importante	No	No	7.8
CVE-2022-35760	Vulnerabilidad de elevación de privilegios en el controlador de puerto ATA de Microsoft	Importante	No	No	7.8
CVE-2022-35762	Vulnerabilidad de elevación directa de privilegios en espacios de almacenamiento	Importante	No	No	7.8
CVE-2022-35763	Vulnerabilidad de elevación directa de privilegios en espacios de almacenamiento	Importante	No	No	7.8
CVE-2022-35764	Vulnerabilidad de elevación directa de privilegios en espacios de almacenamiento	Importante	No	No	7.8
CVE-2022-35765	Vulnerabilidad de elevación directa de privilegios en espacios de almacenamiento	Importante	No	No	7.8
CVE-2022-35792	Vulnerabilidad de elevación directa de privilegios en espacios de almacenamiento	Importante	No	No	7.8
CVE-2022-35773	Vulnerabilidad de ejecución remota de código en	Importante	No	No	7.8

	Azure RTOS GUIX Studio				
CVE-2022-34303	CERT/CC: CVE-20220-34303 Bypass del cargador de arranque Crypto Pro	Importante	No	No	7.8
CVE-2022-34301	CERT/CC: CVE-2022-34301 Derivación del cargador de arranque Eurosoft	Importante	No	No	7.8
CVE-2022-34705	Vulnerabilidad de elevación de privilegios de Credential Guard en Windows Defender	Importante	No	No	7.8
CVE-2022-35768	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2022-35795	Vulnerabilidad de elevación de privilegios en el servicio informe de errores de Windows	Importante	No	No	7.8
CVE-2022-35771	Vulnerabilidad de elevación de privilegios de Credential Guard en Windows Defender	Importante	No	No	7.8
CVE-2022-35779	Vulnerabilidad de ejecución remota de código en Azure RTOS GUIX Studio	Importante	No	No	7.8
CVE-2022-35806	Vulnerabilidad de ejecución remota de código en Azure RTOS GUIX Studio	Importante	No	No	7.8

CVE-2022-35820	Vulnerabilidad de elevación de privilegios en el controlador Bluetooth de Windows	Importante	No	No	7.8
CVE-2022-30134	Vulnerabilidad de divulgación de información en Microsoft Exchange	Importante	Sí	No	7.6
CVE-2022-34302	CERT/CC: CVE-2022-34302 New Horizon Data Systems Inc Bypass del cargador de arranque	Importante	No	No	7.6
CVE-2022-30144	Vulnerabilidad de ejecución remota de código en el servicio Bluetooth de Windows	Importante	No	No	7.5
CVE-2022-30194	Vulnerabilidad de ejecución remota de código en el control de Windows WebBrowser	Importante	No	No	7.5
CVE-2022-35742	Vulnerabilidad de denegación de servicio en Microsoft Outlook	Importante	No	No	7.5
CVE-2022-35748	HTTP.sys Vulnerabilidad de denegación de servicio	Importante	No	No	7.5
CVE-2022-35769	Vulnerabilidad de denegación de servicio en el Protocolo punto a punto (PPP) de Windows	Importante	No	No	7.5
CVE-2022-35755	Vulnerabilidad de elevación de	Importante	No	No	7.3

	privilegios en la cola de impresión de Windows				
CVE-2022-35757	Vulnerabilidad de elevación de privilegios en el controlador de mini filtro de archivos de nube de Windows	Importante	No	No	7.3
CVE-2022-33631	Vulnerabilidad de omisión de la característica de seguridad de Microsoft Excel	Importante	No	No	7.3
CVE-2022-35793	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	No	No	7.3
CVE-2022-35772	Vulnerabilidad de ejecución remota de código en Azure Site Recovery	Importante	No	No	7.2
CVE-2022-35824	Vulnerabilidad de ejecución remota de código en Azure Site Recovery	Importante	No	No	7.2
CVE-2022-34690	Vulnerabilidad de elevación de privilegios en el servicio de fax de Windows	Importante	No	No	7.1
CVE-2022-35754	Vulnerabilidad de elevación de privilegios en el filtro de escritura unificado	Importante	No	No	6.7
CVE-2022-35759	Vulnerabilidad de denegación de servicio de la Autoridad de seguridad local (LSA) de Windows	Importante	No	No	6.5

CVE-2022-35780	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35781	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35799	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35775	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35801	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35807	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35808	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35782	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35809	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35784	Vulnerabilidad de elevación de	Importante	No	No	6.5

	privilegios en Azure Site Recovery				
CVE-2022-35810	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35811	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35785	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35786	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35813	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35788	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35814	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35789	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35815	Vulnerabilidad de elevación de privilegios en	Importante	No	No	6.5

	Azure Site Recovery				
CVE-2022-35790	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35816	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35817	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35791	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35818	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35819	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	6.5
CVE-2022-35776	Vulnerabilidad de denegación de servicio de Azure Site Recovery	Importante	No	No	6.2
CVE-2022-35797	Vulnerabilidad de omisión de la característica de seguridad de Windows Hello	Important	No	No	6.1
CVE-2022-34709	Vulnerabilidad de omisión de la característica de seguridad de Credential Guard	Importante	No	No	6.0

	de Windows Defender				
CVE-2022-35747	Vulnerabilidad de denegación de servicio en el Protocolo punto a punto (PPP) de Windows	Importante	No	No	5.9
CVE-2022-34716	Vulnerabilidad de suplantación de identidad en .NET	Importante	No	No	5.9
CVE-2022-30197	Vulnerabilidad de divulgación de información en el kernel de Windows	Importante	No	No	5.5
CVE-2022-34685	Vulnerabilidad de divulgación de información en Azure RTOS GUIX Studio	Importante	No	No	5.5
CVE-2022-34686	Vulnerabilidad de divulgación de información en Azure RTOS GUIX Studio	Importante	No	No	5.5
CVE-2022-34708	Vulnerabilidad de divulgación de información en el kernel de Windows	Importante	No	No	5.5
CVE-2022-34710	Vulnerabilidad de divulgación de información de Credential Guard en Windows Defender	Importante	No	No	5.5
CVE-2022-34712	Vulnerabilidad de divulgación de información de Credential Guard en Windows Defender	Importante	No	No	5.5
CVE-2022-35758	Vulnerabilidad de divulgación de información de memoria en el	Importante	No	No	5.5

	kernel de Windows				
CVE-2022-34704	Vulnerabilidad de divulgación de información de Credential Guard en Windows Defender	Importante	No	No	5.5
CVE-2022-34692	Vulnerabilidad de divulgación de información en Microsoft Exchange	Importante	No	No	5.3
CVE-2022-34701	Vulnerabilidad de denegación de servicio en el Protocolo de túnel de sockets seguros de Windows (SSTP)	Importante	No	No	5.3
CVE-2022-35774	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	4.9
CVE-2022-35800	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	4.9
CVE-2022-35787	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	4.9
CVE-2022-21979	Vulnerabilidad de divulgación de información en Microsoft Exchange	Importante	No	No	4.8
CVE-2022-35783	Vulnerabilidad de elevación de privilegios en Azure Site Recovery	Importante	No	No	4.4
CVE-2022-35812	Vulnerabilidad de elevación de	Importante	No	No	4.4

	privilegios en Azure Site Recovery				
CVE-2022-35821	Vulnerabilidad de divulgación de información en Azure Sphere	Importante	No	No	4.4
CVE-2022-35796	Microsoft Edge (basado en Chromium) Vulnerabilidad de elevación de privilegios	Baja	No	No	7.5
CVE-2022-33636	Microsoft Edge (basado en Chromium) Vulnerabilidad de ejecución remota de código	Moderada	No	No	8.3
CVE-2022-2603	Chromium Uso después de la liberación en Omnibox	Sin valor asignado	No	No	8.8
CVE-2022-2604	Chromium Uso después de gratis en Navegación Segura	Sin valor asignado	No	No	8.8
CVE-2022-2605	Chromium: CVE-2022-2605 Out of bounds read in Dawn	Sin valor asignado	No	No	8.8
CVE-2022-2606	Chromium Uso después de la liberación en la API de dispositivos administrados	Sin valor asignado	No	No	8.8
CVE-2022-2610	Chromium Aplicación de directivas insuficiente en la captura en segundo plano	Sin valor asignado	No	No	8.8
CVE-2022-2611	Chromium Implementación inapropiada en la	Sin valor asignado	No	No	8.8

	API de pantalla completa				
CVE-2022-2612	Chromium Fuga de información de canal lateral en la entrada del teclado	Sin valor asignado	No	No	8.8
CVE-2022-2614	Chromium Uso después de la liberación en el flujo de inicio de sesión	Sin valor asignado	No	No	8.8
CVE-2022-2615	Chromium Aplicación insuficiente de la política de cookies	Sin valor asignado	No	No	8.8
CVE-2022-2616	Chromium Implementación inadecuada en la API de extensiones	Sin valor asignado	No	No	8.8
CVE-2022-2617	Chromium Uso después de la liberación en extensiones API	Sin valor asignado	No	No	8.8
CVE-2022-2618	Chromium Validación insuficiente de entradas que no son de confianza en Internals	Sin valor asignado	No	No	8.8
CVE-2022-2619	Chromium Validación insuficiente de entradas que no son de confianza en Configuración	Sin valor asignado	No	No	8.8
CVE-2022-2621	Chromium Uso después de la liberación en Extensiones	Sin valor asignado	No	No	8.8
CVE-2022-2622	Chromium Validación insuficiente de la entrada que no	Sin valor asignado	No	No	8.8

	es de confianza en la navegación segura				
CVE-2022-2623	Chromium Uso después de gratis en Offline	Sin valor asignado	No	No	8.8
CVE-2022-2624	Chromium Desbordamiento del búfer del Heap en PDF	Sin valor asignado	No	No	8.8

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

- August 2022 Security Updates
- Security Update Guide - Microsoft
- Zero Day initiative-The August 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