Basque CyberSecurity Centre

Actualización de seguridad de Microsoft-Enero 2023

BCSC-ACTUALIZACIONES-MICROSOFT-2023-ENERO

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Resumen ejecutivo

Microsoft ha publicado las actualizaciones de seguridad del mes de enero de 2023. Con estas actualizaciones se corrigen 98 vulnerabilidades, siendo 11 de ellas calificadas como críticas y 87 como importantes.

Hay que destacar que dentro de ellas hay **2 zero-day**, **una siendo explotada (CVE-2023-21674) y otra que ha sido divulgada públicamente (CVE-2023-21549).**

Estas vulnerabilidades afectan a productos como Windows Point-to-Point Tunneling Protocol, Microsoft Office SharePoint, Windows Authentication Methods, Windows Cryptographic Services y Windows Layer 2 Tunneling Protocol, entre otros.

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

- 4 vulnerabilidad de bypass.
- 10 vulnerabilidades de denegación de servicio.
- 10 vulnerabilidades de divulgación de información.
- 33 vulnerabilidades de ejecución remota de código.
- 39 vulnerabilidades de elevación de privilegios.
- 2 vulnerabilidades de spoofing.

2. Recursos afectados

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

- .NET Core
- 3D Builder
- Azure Service Fabric Container
- Microsoft Bluetooth Driver
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Local Security Authority Server (lsasrv)
- Microsoft Message Queuing
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft WDAC OLE DB provider for SQL
- Visual Studio Code
- Windows ALPC
- Windows Ancillary Function Driver for WinSock
- Windows Authentication Methods
- Windows Backup Engine
- Windows Bind Filter Driver
- Windows BitLocker
- Windows Boot Manager
- Windows Credential Manager
- Windows Cryptographic Services
- Windows DWM Core Library
- Windows Error Reporting
- Windows Event Tracing
- Windows IKE Extension
- Windows Installer
- Windows Internet Key Exchange (IKE) Protocol

- Windows iSCSI
- Windows Kernel
- Windows Layer 2 Tunneling Protocol
- Windows LDAP - Lightweight Directory Access Protocol
- Windows Local Security Authority (LSA)
- Windows Local Session Manager (LSM)
- Windows Malicious Software Removal Tool
- Windows Management Instrumentation
- Windows MSCryptDImportKey
- Windows NTLM
- Windows ODBC Driver
- Windows Overlay Filter
- Windows Point-to-Point Tunneling Protocol
- Windows Print Spooler Components
- Windows Remote Access Service L2TP Driver
- Windows RPC API
- Windows Secure Socket Tunneling Protocol (SSTP)
- Windows Smart Card
- Windows Task Scheduler
- Windows Virtual Registry Provider
- Windows Workstation Service

3. Análisis técnico

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

Las 2 vulnerabilidades zero-day tratadas son:

CVE-2023-21674: vulnerabilidad de elevación de privilegios en la llamada al procedimiento local avanzado (ALPC) de Windows. El fallo podría conducir a un escape de sandbox del navegador, de forma que, un atacante que aprovechara con éxito esta vulnerabilidad podría obtener privilegios de SISTEMA. Desde Microsoft se sabe que **este fallo está siendo explotado en la actualidad**.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.8

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

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

CVE-2023-21549: vulnerabilidad de elevación de privilegios del servicio testigo SMB de Windows. Para aprovechar esta vulnerabilidad, un atacante podría ejecutar un script malicioso especialmente diseñado que ejecute una llamada RPC a un host RPC. Esto podría resultar en una elevación de privilegios en el servidor. Consecuentemente, dicho atacante que aprovechara con éxito esta vulnerabilidad podría ejecutar funciones RPC que estén restringidas, pero solo a cuentas con privilegios. Remarcar que **el fallo ha sido divulgado publicamente**.

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

Las vulnerabilidades críticas corregidas son:

CVE-2023-21561: vulnerabilidad de elevación de privilegios de los servicios criptográficos de Microsoft. Un atacante autenticado localmente podría enviar datos especialmente diseñados al servicio CSRSS local para elevar sus privilegios de AppContainer a SYSTEM. Debido a que el entorno de AppContainer se considera un límite de seguridad defendible, cualquier proceso que pueda eludir el límite se considera un cambio en el Ámbito. El atacante podría entonces ejecutar código o acceder a recursos a un nivel de integridad más alto que el del entorno de ejecución de AppContainer.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.8

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

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

CVE-2023-21535: vulnerabilidad de ejecución remota de código del protocolo de túnel de sockets seguros (SSTP) 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-2023-21546: vulnerabilidad de ejecución remota de código del protocolo de tunelización de capa 2 (L2TP) 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: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-21543: vulnerabilidad de ejecución remota de código del protocolo de tunelización de capa 2 (L2TP) 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: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-21548: vulnerabilidad de ejecución remota de código del protocolo de túnel de sockets seguros (SSTP) de Windows. Para aprovechar esta vulnerabilidad, un atacante necesitaría enviar un paquete SSTP malicioso especialmente diseñado a un servidor SSTP. 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-2023-21555: vulnerabilidad de ejecución remota de código del protocolo de tunelización de capa 2 (L2TP) 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-2023-21556: vulnerabilidad de ejecución remota de código del protocolo de tunelización de capa 2 (L2TP) 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-2023-21679: vulnerabilidad de ejecución remota de código del protocolo de tunelización de capa 2 (L2TP) 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-2023-21551: vulnerabilidad de elevación de privilegios de los servicios criptográficos de Microsoft. Un atacante que explotara con éxito esta vulnerabilidad podría obtener privilegios de SISTEMA

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**: **Bajo**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-21730: vulnerabilidad de elevación de privilegios de los servicios criptográficos de Microsoft. Un atacante que explotara con éxito esta vulnerabilidad podría obtener privilegios de SISTEMA.

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**: **Bajo**

- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-21743: vulnerabilidad de omisión de la característica de seguridad de Microsoft SharePoint Server, de manera que en un ataque basado en la red, un atacante no autenticado podría pasar por alto la autenticación y establecer una conexión anónima, ya que, el atacante puede eludir el acceso de usuario esperado como un usuario no autenticado.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 5.3

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

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

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

CVE	Descripción	Severidad	Divulgado	Explotado	CVSS
CVE-2023-21561	Vulnerabilidad de elevación de privilegios en los servicios criptográficos de Microsoft	**Crítica**	No	No	8.8
CVE-2023-21535	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets seguros (SSTP) en Windows	**Crítica**	No	No	8.1
CVE-2023-21546	Vulnerabilidad de ejecución remota de código en el	**Crítica**	No	No	8.1

	Protocolo de túnel de capa 2 (L2TP) en Windows				
CVE-2023-21543	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de capa 2 (L2TP) en Windows	**Crítica**	No	No	8.1
CVE-2023-21548	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets seguros (SSTP) en Windows	**Crítica**	No	No	8.1
CVE-2023-21555	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de capa 2 (L2TP) en Windows	**Crítica**	No	No	8.1
CVE-2023-21556	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de capa 2 (L2TP) en Windows	**Crítica**	No	No	8.1
CVE-2023-21679	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de capa 2 (L2TP) en Windows	**Crítica**	No	No	8.1
CVE-2023-21551	Vulnerabilidad de elevación de privilegios en	**Crítica**	No	No	7.8

	los servicios criptográficos de Microsoft				
CVE-2023-21730	Vulnerabilidad de elevación de privilegios en los servicios criptográficos de Microsoft	**Crítica**	No	No	7.8
CVE-2023-21743	Vulnerabilidad de omisión de la característica de seguridad de Microsoft SharePoint Server	**Crítica**	No	No	5.3
CVE-2023-21549	Vulnerabilidad de elevación de privilegios en el servicio testigo SMB de Windows	Importante	Sí	No	8.8
CVE-2023-21674	Vulnerabilidad de elevación de privilegios en Windows Advanced Local Procedure Call (ALPC)	Importante	No	Sí	8.8
CVE-2023-21676	Vulnerabilidad de ejecución remota de código en el Protocolo ligero de acceso a directorios (LDAP) en Windows	Importante	No	No	8.8
CVE-2023-21681	Vulnerabilidad de ejecución remota de código en el proveedor OLE DB de Microsoft WDAC para SQL Server	Importante	No	No	8.8

CVE-2023-21732	Vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft	Importante	No	No	8.8
CVE-2023-21742	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	Importante	No	No	8.8
CVE-2023-21744	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	Importante	No	No	8.8
CVE-2023-21762	Vulnerabilidad de suplantación de identidad en Microsoft Exchange Server	Importante	No	No	8.0
CVE-2023-21745	Vulnerabilidad de suplantación de identidad en Microsoft Exchange Server	Importante	No	No	8.0
CVE-2023-21524	Vulnerabilidad de elevación de privilegios de la autoridad de seguridad local (LSA) de Windows	Importante	No	No	7.8
CVE-2023-21541	Vulnerabilidad de elevación de privilegios en el Programador de tareas de Windows	Importante	No	No	7.8
CVE-2023-21552	Vulnerabilidad de elevación de	Importante	No	No	7.8

	privilegios en la GDI de Windows				
CVE-2023-21558	Vulnerabilidad de elevación de privilegios en el servicio Informe de errores de Windows	Importante	No	No	7.8
CVE-2023-21678	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	No	No	7.8
CVE-2023-21680	Vulnerabilidad de elevación de privilegios en Windows Win32k	Importante	No	No	7.8
CVE-2023-21724	Vulnerabilidad de elevación de privilegios en la biblioteca principal de Microsoft DWM	Importante	No	No	7.8
CVE-2023-21726	Vulnerabilidad de elevación de privilegios en la interfaz de usuario del Administrador de credenciales de Windows	Importante	No	No	7.8
CVE-2023-21734	Vulnerabilidad de ejecución remota de código en Microsoft Office	Importante	No	No	7.8
CVE-2023-21735	Vulnerabilidad de ejecución remota de código en Microsoft Office	Importante	No	No	7.8
CVE-2023-21736	Vulnerabilidad de ejecución remota de código en	Importante	No	No	7.8

	Microsoft Office Visio				
CVE-2023-21737	Vulnerabilidad de ejecución remota de código en Microsoft Office Visio	Importante	No	No	7.8
CVE-2023-21746	Vulnerabilidad de elevación de privilegios en NTLM en Windows	Importante	No	No	7.8
CVE-2023-21747	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2023-21748	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2023-21749	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2023-21754	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2023-21755	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2023-21763	Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server	Importante	No	No	7.8
CVE-2023-21764	Vulnerabilidad de elevación de privilegios en	Importante	No	No	7.8

	Microsoft Exchange Server				
CVE-2023-21765	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	No	No	7.8
CVE-2023-21767	Vulnerabilidad de elevación de privilegios en el filtro de superposición de Windows	Importante	No	No	7.8
CVE-2023-21768	Controlador de función auxiliar de Windows para la vulnerabilidad de elevación de privilegios en WinSock	Importante	No	No	7.8
CVE-2023-21772	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2023-21773	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2023-21774	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2023-21780	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8
CVE-2023-21781	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8

CVE-2023-21782	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8
CVE-2023-21784	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8
CVE-2023-21786	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8
CVE-2023-21791	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8
CVE-2023-21793	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8
CVE-2023-21537	Vulnerabilidad de elevación de privilegios en Microsoft Message Queue Server (MSMQ)	Importante	No	No	7.8
CVE-2023-21675	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2023-21783	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8
CVE-2023-21785	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8

CVE-2023-21787	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8
CVE-2023-21788	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8
CVE-2023-21789	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8
CVE-2023-21790	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8
CVE-2023-21792	Vulnerabilidad de ejecución remota de código en 3D Builder	Importante	No	No	7.8
CVE-2023-21538	Vulnerabilidad de denegación de servicio en .NET	Importante	No	No	7.5
CVE-2023-21547	Vulnerabilidad de denegación de servicio en el protocolo de intercambio de claves de Internet (IKE)	Importante	No	No	7.5
CVE-2023-21539	Vulnerabilidad de ejecución remota de código en la autenticación de Windows	Importante	No	No	7.5
CVE-2023-21557	Vulnerabilidad de denegación de servicio del Protocolo ligero de acceso a	Importante	No	No	7.5

	directorios (LDAP) en Windows				
CVE-2023-21677	Vulnerabilidad de denegación de servicio en la extensión de intercambio de claves Internet (IKE) en Windows	Importante	No	No	7.5
CVE-2023-21683	Vulnerabilidad de denegación de servicio en la extensión de intercambio de claves Internet (IKE) en Windows	Importante	No	No	7.5
CVE-2023-21728	Vulnerabilidad de denegación de servicio en Windows Netlogon	Importante	No	No	7.5
CVE-2023-21757	Vulnerabilidad de denegación de servicio del Protocolo de túnel de capa 2 (L2TP) de Windows	Importante	No	No	7.5
CVE-2023-21758	Vulnerabilidad de denegación de servicio en la extensión de intercambio de claves Internet (IKE) en Windows	Importante	No	No	7.5
CVE-2023-21761	Vulnerabilidad de divulgación de información en Microsoft Exchange Server	Importante	No	No	7.5
CVE-2023-21527	Vulnerabilidad de denegación de servicio en	Importante	No	No	7.5

	iSCSI en Windows				
CVE-2023-21779	Ejecución remota de código de Visual Studio Code	Importante	No	No	7.3
CVE-2023-21738	Vulnerabilidad de ejecución remota de código en Microsoft Office Visio	Importante	No	No	7.1
CVE-2023-21741	Vulnerabilidad de divulgación de información en Microsoft Office Visio	Importante	No	No	7.1
CVE-2023-21750	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.1
CVE-2023-21752	Vulnerabilidad de elevación de privilegios en el servicio de copia de seguridad de Windows	Importante	No	No	7.1
CVE-2023-21760	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	No	No	7.1
CVE-2023-21532	Vulnerabilidad de elevación de privilegios en la GDI de Windows	Importante	No	No	7.0
CVE-2023-21542	Vulnerabilidad de elevación de privilegios en Windows Installer	Importante	No	No	7.0
CVE-2023-21733	Vulnerabilidad de elevación de privilegios en el	Importante	No	No	7.0

	controlador de filtro de enlace de Windows				
CVE-2023-21739	Vulnerabilidad de elevación de privilegios en el controlador Bluetooth de Windows	Importante	No	No	7.0
CVE-2023-21771	Vulnerabilidad de elevación de privilegios en el Administrador de sesiones locales (LSM) en Windows	Importante	No	No	7.0
CVE-2023-21531	Vulnerabilidad de elevación de privilegios en contenedores de Azure Service Fabric	Importante	No	No	7.0
CVE-2023-21563	Vulnerabilidad de omisión de la característica de seguridad de BitLocker	Importante	No	No	6.8
CVE-2023-21560	Vulnerabilidad de omisión de la característica de seguridad del Administrador de arranque de Windows	Importante	No	No	6.6
CVE-2023-21725	Vulnerabilidad de elevación de privilegios de la herramienta de eliminación de software malintencionado de Windows	Importante	No	No	6.3
CVE-2023-21540	Vulnerabilidad de divulgación de información criptográfica en Windows	Importante	No	No	5.5

CVE-2023-21550	Vulnerabilidad de divulgación de información criptográfica en Windows	Importante	No	No	5.5
CVE-2023-21559	Vulnerabilidad de divulgación de información criptográfica en Windows	Importante	No	No	5.5
CVE-2023-21753	Seguimiento de eventos para la vulnerabilidad de divulgación de información en Windows	Importante	No	No	5.5
CVE-2023-21776	Vulnerabilidad de divulgación de información en el kernel de Windows	Importante	No	No	5.5
CVE-2023-21682	Vulnerabilidad de divulgación de información en el Protocolo punto a punto (PPP) de Windows	Importante	No	No	5.3
CVE-2023-21525	Vulnerabilidad de denegación de servicio en tiempo de ejecución en tiempo de ejecución de llamada a procedimiento remoto	Importante	No	No	5.3
CVE-2023-21766	Vulnerabilidad de divulgación de información en el filtro de superposición de Windows	Importante	No	No	4.7
CVE-2023-21536	Seguimiento de eventos para la vulnerabilidad	Importante	No	No	4.7

	de divulgación de información en Windows				
CVE-2023-21759	Vulnerabilidad de omisión de la característica de seguridad del servidor de administración de recursos de tarjetas inteligentes de Windows	Importante	No	No	3.3

4. Mitigación / Solución

Para la mitigación y la corrección de todas las vulnerabilidades, Microsoft publica las actualizaciones de seguridad pertinentes junto con sus release notes, las cuales están disponibles en Security Update Guide.

5. Referencias Adicionales

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


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA