Basque CyberSecurity Centre

Actualización de seguridad de Microsoft-Septiembre 2022

BCSC-ACTUALIZACIONES-MICROSOFT-2022-SEPTIEMBRE

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 septiembre de 2022. Con estas actualizaciones se corrigen 64 vulnerabilidades, siendo 5 de ellas calificadas como críticas, 58 como importantes y 1 baja. A estas vulnerabilidades hay que añadir otras 15 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 and Visual Studio, .NET Framework, Windows Kernel, Microsoft Office, Microsoft Office SharePoint, Windows Defender, Windows Distributed File System (DFS) y Windows TCP/IP entre otros.

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

- 1 vulnerabilidad de bypass.
- 7 vulnerabilidades de denegación de servicio
- 6 vulnerabilidades de divulgación de información.
- 31 vulnerabilidades de ejecución remota de código.
- 18 vulnerabilidades de elevación de privilegios.
- 1 vulnerabilidad de restricción de especulación de caché que afecta a ciertos procesadores Arm Cortex y Neoverse.

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:

- .NET and Visual Studio
- .NET Framework
- Azure Arc
- Cache Speculation
- HTTP.sys
- Microsoft Dynamics
- Microsoft Edge (Chromium-based)
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft Windows ALPC
- Microsoft Windows Codecs Library
- Network Device Enrollment Service (NDES)
- Role: DNS Server
- Role: Windows Fax Service
- SPNEGO Extended Negotiation
- Visual Studio Code
- Windows Common Log File System Driver
- Windows Credential Roaming Service
- Windows Defender
- Windows Distributed File System (DFS)
- Windows DPAPI (Data Protection Application Programming Interface)
- Windows Enterprise App Management
- Windows Event Tracing
- Windows Group Policy
- Windows IKE Extension

- Windows Kerberos
- Windows Kernel
- Windows LDAP - Lightweight Directory Access Protocol
- Windows ODBC Driver
- Windows OLE
- Windows Photo Import API
- Windows Print Spooler Components
- Windows Remote Access Connection Manager
- Windows Remote Procedure Call
- Windows TCP/IP
- Windows Transport Security Layer (TLS)

3. Análisis técnico

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

CVE-2022-23960: vulnerabilidad de restricción de especulación de caché que afecta a ciertos procesadores Arm Cortex y Neoverse hasta el 2022-03-08 y que **ha sido divulgada públicamente**. Estos procesadores no restringen adecuadamente la especulación de caché, también conocido como Spectre-BHB, de forma que un atacante puede aprovechar el historial de sucursales compartido en el búfer (BHB) para influir en las sucursales mal pronosticadas, de manera que la asignación de caché puede permitir que el atacante obtenga información confidencial del sistema.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 5.6

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

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

CVE-2022-37969: vulnerabilidad de elevación de privilegios del controlador del sistema de archivo de registro común de Windows, de forma que un atacante que aprovechara con éxito esta vulnerabilidad podría obtener privilegios de sistema. **Remarcar que la vulnerabilidad ha sido divulgada públicamente y está siendo explotada.**

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.8

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

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

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

CVE-2022-34718: vulnerabilidad de ejecución remota de código TCP/IP de Windows, de manera que un atacante no autenticado podría enviar un paquete IPv6 especialmente diseñado a un nodo de Windows donde IPSec esté habilitado, lo que podría permitir una explotación de ejecución remota de código en esa máquina.

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-2022-34721: vulnerabilidad de ejecución remota de código en extensiones de protocolo de intercambio de claves de Internet (IKE) de Windows, de forma que un atacante no autenticado podría enviar un paquete IP especialmente diseñado a una máquina de destino que ejecuta Windows y tenga IPSec habilitado, lo que podría permitir una explotación de ejecución remota de código.

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-2022-34722: vulnerabilidad de ejecución remota de código en extensiones de protocolo de intercambio de claves de Internet (IKE) de Windows, de manera que, un atacante no autenticado podría enviar un paquete IP especialmente

diseñado a una máquina de destino que ejecuta Windows y tenga IPSec habilitado, lo que podría permitir una explotación de ejecución remota de código.

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-2022-35805: vulnerabilidad de ejecución remota de código de Microsoft Dynamics CRM (local), de forma que, un usuario autenticado podría ejecutar un paquete confiable especialmente diseñado para ejecutar comandos SQL arbitrarios. Desde ahí, el atacante podría escalar y ejecutar comandos como db_owner dentro de su base de datos de Dynamics 365.

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-2022-34700: vulnerabilidad de ejecución remota de código de Microsoft Dynamics CRM (local), de manera que, un usuario autenticado podría ejecutar un paquete confiable especialmente diseñado para ejecutar comandos SQL arbitrarios. Una vez en este punto, el atacante podría escalar y ejecutar comandos como db_owner dentro de su base de datos de Dynamics 365.

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**

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

CVE	Descripción	Severidad	Divulgado	Explotado	CVSS
CVE-2022-34718	Vulnerabilidad de ejecución remota de código TCP/IP en Windows	**Crítica**	No	No	9.8
CVE-2022-34721	Vulnerabilidad de ejecución remota de código en las extensiones de protocolo de intercambio de claves de Internet (IKE) de Windows	**Crítica**	No	No	9.8
CVE-2022-34722	Vulnerabilidad de ejecución remota de código en las extensiones de protocolo de intercambio de claves de Internet (IKE) de Windows	**Crítica**	No	No	9.8
CVE-2022-35805	Vulnerabilidad de ejecución remota de código en Microsoft Dynamics CRM (local)	**Crítica**	No	No	8.8
CVE-2022-34700	Vulnerabilidad de ejecución remota de	**Crítica**	No	No	8.8

	código en Microsoft Dynamics CRM (local)				
CVE-2022-38008	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	Importante	No	No	8.8
CVE-2022-38009	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	Importante	No	No	8.8
CVE-2022-37961	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	Importante	No	No	8.8
CVE-2022-35834	Vulnerabilidad de ejecución remota de código en el proveedor OLE DB de Microsoft para SQL Server	Importante	No	No	8.8
CVE-2022-35835	Vulnerabilidad de ejecución remota de código en el proveedor OLE DB de Microsoft para SQL Server	Importante	No	No	8.8
CVE-2022-35836	Vulnerabilidad de ejecución remota de código en el proveedor OLE DB de Microsoft para SQL Server	Importante	No	No	8.8

CVE-2022-35840	Vulnerabilidad de ejecución remota de código en el proveedor OLE DB de Microsoft para SQL Server	Importante	No	No	8.8
CVE-2022-35841	Vulnerabilidad de ejecución remota de código en el Servicio de administración de aplicaciones de Windows Enterprise	Importante	No	No	8.8
CVE-2022-34726	Vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft	Importante	No	No	8.8
CVE-2022-34727	Vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft	Importante	No	No	8.8
CVE-2022-34730	Vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft	Importante	No	No	8.8
CVE-2022-34731	Vulnerabilidad de ejecución remota de código en el proveedor OLE DB de Microsoft para SQL Server	Importante	No	No	8.8
CVE-2022-34732	Vulnerabilidad de ejecución remota de	Importante	No	No	8.8

	código en el controlador ODBC de Microsoft				
CVE-2022-34733	Vulnerabilidad de ejecución remota de código en el proveedor OLE DB de Microsoft para SQL Server	Importante	No	No	8.8
CVE-2022-34734	Vulnerabilidad de ejecución remota de código en el controlador ODBC de Microsoft	Importante	No	No	8.8
CVE-2022-30196	Vulnerabilidad de denegación de servicio en el canal seguro de Windows	Importante	No	No	8.2
CVE-2022-33679	Vulnerabilidad de elevación de privilegios en Kerberos de Windows	Importante	No	No	8.1
CVE-2022-35823	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint	Importante	No	No	8.1
CVE-2022-33647	Vulnerabilidad de elevación de privilegios en Kerberos de Windows	Importante	No	No	8.1
CVE-2022-35830	Vulnerabilidad de ejecución remota de código en tiempo de ejecución remota en tiempo de	Importante	No	No	8.1

	ejecución de llamadas a procedimientos remotos				
CVE-2022-26929	Vulnerabilidad de ejecución remota de código en .NET Framework	Importante	No	No	7.8
CVE-2022-35803	Vulnerabilidad de elevación de privilegios en el controlador del sistema de archivos de registro común de Windows	Importante	No	No	7.8
CVE-2022-35828	Vulnerabilidad de elevación de privilegios en Microsoft Defender para Endpoint para Mac	Importante	No	No	7.8
CVE-2022-37964	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2022-30200	Vulnerabilidad de ejecución remota de código en el Protocolo ligero de acceso a directorios (LDAP) de Windows	Importante	No	No	7.8
CVE-2022-34719	Vulnerabilidad de elevación de privilegios en el sistema de archivos distribuido (DFS) de Windows	Importante	No	No	7.8

CVE-2022-34729	Vulnerabilidad de elevación de privilegios en Windows GDI	Importante	No	No	7.8
CVE-2022-37954	Vulnerabilidad de elevación de privilegios en el kernel de gráficos DirectX	Importante	No	No	7.8
CVE-2022-37955	Vulnerabilidad de elevación de privilegios en la directiva de grupo de Windows	Importante	No	No	7.8
CVE-2022-37956	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2022-38004	Vulnerabilidad de ejecución remota de código en el servicio de fax de Windows	Importante	No	No	7.8
CVE-2022-37957	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2022-38005	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	No	No	7.8
CVE-2022-38007	Vulnerabilidad de elevación de privilegios en la configuración de invitados de Azure y los servidores habilitados para Azure Arc	Importante	No	No	7.8

CVE-2022-38010	Vulnerabilidad de ejecución remota de código en Microsoft Office Visio	Importante	No	No	7.8
CVE-2022-37962	Vulnerabilidad de ejecución remota de código en Microsoft PowerPoint	Importante	No	No	7.8
CVE-2022-37963	Vulnerabilidad de ejecución remota de código en Microsoft Office Visio	Importante	No	No	7.8
CVE-2022-23960	Arm: Vulnerabilidad de restricción de especulación de caché	Importante	Sí	No	7.8
CVE-2022-37969	Vulnerabilidad de elevación de privilegios en el controlador del sistema de archivos de registro común de Windows	Importante	Sí	Sí	7.8
CVE-2022-38019	Vulnerabilidad de ejecución remota de código en la extensión de vídeo AV1	Importante	No	No	7.8
CVE-2022-38013	Vulnerabilidad de denegación de servicio en .NET Core y Visual Studio	Importante	No	No	7.5
CVE-2022-35833	Vulnerabilidad de denegación de servicio en el	Importante	No	No	7.5

	canal seguro de Windows				
CVE-2022-35838	Vulnerabilidad de denegación de servicio http V3	Importante	No	No	7.5
CVE-2022-34720	Vulnerabilidad de denegación de servicio en la extensión de intercambio de claves de Internet (IKE) de Windows	Importante	No	No	7.5
CVE-2022-34724	Vulnerabilidad de denegación de servicio en windows DNS Server	Importante	No	No	7.5
CVE-2022-37958	Vulnerabilidad de divulgación de información del mecanismo de negociación extendida de SPNEGO (NEGOEX)	Importante	No	No	7.5
CVE-2022-30170	Vulnerabilidad de elevación de privilegios en el servicio móvil de credenciales de Windows	Importante	No	No	7.3
CVE-2022-38011	Vulnerabilidad de ejecución remota de código en la extensión de imagen sin procesar	Importante	No	No	7.3
CVE-2022-38020	Vulnerabilidad de elevación de privilegios en Visual Studio Code	Importante	No	No	7.3

CVE-2022-26928	Vulnerabilidad de elevación de privilegios en la API de importación de fotos de Windows	Importante	No	No	7.0
CVE-2022-34725	Vulnerabilidad de elevación de privilegios en Windows ALPC	Importante	No	No	7.0
CVE-2022-38006	Vulnerabilidad de divulgación de información de componentes de gráficos de Windows	Importante	No	No	6.5
CVE-2022-37959	Vulnerabilidad de omisión de la característica de seguridad del Servicio de inscripción de dispositivos de red (NDES)	Importante	No	No	6.5
CVE-2022-35831	Vulnerabilidad de divulgación de información en el Administrador de conexiones de acceso remoto de Windows	Importante	No	No	5.5
CVE-2022-35832	Vulnerabilidad de denegación de servicio en el seguimiento de eventos de Windows	Importante	No	No	5.5
CVE-2022-34723	Vulnerabilidad de divulgación de información en DPAPI (interfaz de programación	Importante	No	No	5.5

	de aplicaciones de protección de datos) de Windows DPAPI (Interfaz de programación de aplicaciones de protección de datos)				
CVE-2022-34728	Vulnerabilidad de divulgación de información de componentes de gráficos de Windows	Importante	No	No	5.5
CVE-2022-35837	Vulnerabilidad de divulgación de información de componentes de gráficos de Windows	Importante	No	No	5.0
CVE-2022-38012	Microsoft Edge basado en Chromium Vulnerabilidad de ejecución remota de código	Baja	No	No	7.7
CVE-2022-3038	Chromium: Uso después de la gratuidad en el servicio de red	Sin valor asignado	No	No	7.8
CVE-2022-3039	Chromium: Uso después de la liberación en WebSQL	Sin valor asignado	No	No	7.8
CVE-2022-3040	Chromium: Usar después de la liberación en Layout	Sin valor asignado	No	No	7.8
CVE-2022-3041	Chromium: Uso después de la liberación en WebSQL	Sin valor asignado	No	No	7.8

CVE-2022-3044	Chromium: Implementación inapropiada en el aislamiento del sitio	Sin valor asignado	No	No	7.8
CVE-2022-3045	Chromium: Validación insuficiente de entradas que no son de confianza en V8	Sin valor asignado	No	No	7.8
CVE-2022-3046	Chromium: Uso después de gratis en Browser Tag	Sin valor asignado	No	No	7.8
CVE-2022-3047	Chromium: Aplicación de directivas insuficiente en la API de extensiones	Sin valor asignado	No	No	7.8
CVE-2022-3053	Chromium: Implementación inadecuada en el bloqueo de puntero	Sin valor asignado	No	No	7.8
CVE-2022-3054	Chromium: Aplicación de directivas insuficiente en DevTools	Sin valor asignado	No	No	7.8
CVE-2022-3055	Chromium: Usar después de gratis en Contraseñas	Sin valor asignado	No	No	7.8
CVE-2022-3056	Chromium: Aplicación insuficiente de directivas en la directiva de seguridad de contenido	Sin valor asignado	No	No	7.8
CVE-2022-3057	Chromium: Implementación inapropiada en iframe Sandbox	Sin valor asignado	No	No	7.8

CVE-2022-3058	Chromium: Uso después de la liberación en el flujo de inicio de sesión	Sin valor asignado	No	No	7.8
CVE-2022-3075	Chromium: Validación de datos insuficiente en Mojo	Sin valor asignado	No	No	7.8

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

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