Actualizaciones de Seguridad de Microsoft - Febrero 2022

BCSC-ACTUALIZACIONES-MICROSOFT-2022-FEBRERO

TLP:WHITE

www.basquecybersecurity.eus

Febrero 2022

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:

1. RESUMEN EJECUTIVO

Microsoft ha publicado las actualizaciones de seguridad del mes febrero de 2022. Con estas actualizaciones se corrigen 51 vulnerabilidades, siendo 50 calificadas como importantes y 1 como moderada. Estas vulnerabilidades afectan a productos como Microsoft Teams, Office, Outlook, OneDrive o SQL Server entre otros.

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

- 3 vulnerabilidades de suplantación (spoofing)
- 5 vulnerabilidades de denegación de servicio.
- 5 vulnerabilidades de divulgación de información.
- 16 vulnerabilidades de ejecución remota de código.
- 4 vulnerabilidades de bypass.
- 18 vulnerabilidades de elevación de privilegios.

A estas vulnerabilidades hay que añadir otras 19 corregidas en el navegador Edge basado en Chromium, para las que Microsoft no ha establecido un nivel de severidad.

Desde el BCSCS recomendamos la aplicación de estas actualizaciones en cuanto sea posible.

2. RECURSOS AFECTADOS

Los parches de seguridad de este mes están asociados a vulnerabilidades que afectan a los siguientes productos:

- Azure Data Explorer
- Kestrel Web Server
- Microsoft Dynamics
- Microsoft Dynamics GP
- Microsoft Edge (Chromium-based)
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office Outlook
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft OneDrive
- Microsoft Teams
- Microsoft Windows Codecs Library
- Power BI
- Roaming Security Rights Management Services
- Role: DNS Server
- Role: Windows Hyper-V
- SQL Server
- Visual Studio Code
- Windows Common Log File System Driver
- Windows DWM Core Library
- Windows Kernel
- Windows Kernel-Mode Drivers
- Windows Named Pipe File System
- Windows Print Spooler Components
- Windows Remote Access Connection Manager
- Windows Remote Procedure Call Runtime
- Windows User Account Profile
- Windows Win32K

3. ANÁLISIS TÉCNICO

Las vulnerabilidades más destacables que han sido corregidas en esta actualización son las que tienen el índice CVSS más elevado, por encima de 8 todas ellas. Son las siguientes:

- CVE 2022-22005: Consiste en una vulnerabilidad de ejecución remota de código en Sharepoint, Server. Su explotación es sencilla ya que no requiere condiciones especiales de acceso. Hay que remarcar que el ataque se puede lanzar de forma remota y según la métrica de privilegios requeridos para la explotación de esta vulnerabilidad, sólo es necesaria una autenticación simple por parte del atacante.
- CVE-2022-23274: Al igual que la anterior es una vulnerabilidad de ejecución de código remoto sobre Microsoft Dynamics GP, un software de gestión empresarial. Es posible iniciar un ataque de forma remota, aunque se requiere autenticación en el sistema por parte del agente malicioso para conseguir su explotación.
- CVE-2022-21987: Esta vulnerabilidad es de escalada de privilegios en Microsoft Sharepoint Server 2013 y puede ser explotada a través de la red.
- CVE-2022-21984: Vulnerabilidad de ejecución remota de código en el servidor DNS de Windows, de explotación relativamente sencilla según las métricas aportadas por Microsoft. La explotación necesita de autenticación por parte del atacante en el sistema.
- CVE-2022-21991: Vulnerabilidad de ejecución de código remoto en el componente Remote Development Extensions de Visual Studio. Su explotación es complicada ya que la complejidad de un ataque es alta, implicando que un agente malicioso tiene que invertir tiempo y esfuerzo para explotarla exitosamente.
- CVE-2022-23256: Esta vulnerabilidad de spoofing en el explorador de datos de Azure permite que un ataque se puede lanzar de forma remota y sencilla ya. No es necesaria autenticación para conseguir explotarla exitosamente, pero requiere que la víctima realice alguna acción, a través de métodos de ingeniería social tal vez, para que el agente malicioso consiga su objetivo.

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

CVE	Descripción	Severidad	CVSS
CVE-2022-21971	Vulnerabilidad de ejecución remota de código en Windows en tiempo de ejecución	Importante	7.8
CVE-2022-21986	Vulnerabilidad de denegación de servicio en .NET	Importante	7.5
CVE-2022-21989	Vulnerabilidad de elevación de privilegios en el Kernel de Windows	Importante	7.8
CVE-2022-21991	Vulnerabilidad de ejecución remota de código en la extensión de desarrollo remoto de Visual Studio Code	Importante	8.1
CVE-2022-21992	Vulnerabilidad de ejecución remota de código en administración de dispositivos de Windows Mobile	Importante	7.8
CVE-2022-21993	Vulnerabilidad de divulgación de información del controlador de Servicios de Windows para NFS ONCRPC XDR	Importante	7.5
CVE-2022-21994	Vulnerabilidad de elevación de privilegios en la biblioteca principal de DWM de Windows	Importante	7.8
CVE-2022-21995	Vulnerabilidad de ejecución remota de código en Windows Hyper-V	Importante	7.9
CVE-2022-21997	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	7.1
CVE-2022-21998	Vulnerabilidad de divulgación de información del controlador del sistema de archivos de registro común de Windows	Importante	5.5
CVE-2022-21999	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	7.8

CVE-2022-21985	Vulnerabilidad de divulgación de información en el Administrador de conexiones de acceso remoto de Windows	Importante	5.5
CVE-2022-22000	Vulnerabilidad de elevación de privilegios en el controlador del sistema de archivos de registro común de Windows	Importante	7.8
CVE-2022-22002	Vulnerabilidad de denegación de servicio en la imagen de perfil de la cuenta de usuario de Windows	Importante	5.5
CVE-2022-22003	Vulnerabilidad de ejecución remota de código en Microsoft Office Graphics	Importante	7.8
CVE-2022-22004	Vulnerabilidad de ejecución remota de código ClickToRun en Microsoft Office	Importante	7.8
CVE-2022-22005	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	Importante	8.8
CVE-2022-23252	Vulnerabilidad de divulgación de información en Microsoft Office	Importante	5.5
CVE-2022-23255	Vulnerabilidad de omisión de la característica de seguridad de Microsoft OneDrive para Android	Importante	5.9
CVE-2022-23256	Vulnerabilidad de suplantación de identidad en azure Data Explorer	Importante	8.1
CVE-2022-23262	Vulnerabilidad de elevación de privilegios en Microsoft Edge (basada en Chromium)	Importante	6.3
CVE-2022-23263	Vulnerabilidad de elevación de privilegios en Microsoft Edge (basada en Chromium)	Importante	7.7

CVE-2022-23280	Vulnerabilidad de omisión de la característica de seguridad de Microsoft Outlook para Mac	Importante	5.3
CVE-2022-22001	Vulnerabilidad de elevación de privilegios en el Administrador de conexiones de acceso remoto de Windows	Importante	7.8
CVE-2022-21984	Vulnerabilidad de ejecución remota de código en Windows DNS Server	Importante	8.8
CVE-2022-21996	Vulnerabilidad de elevación de privilegios en Win32k	Importante	7.8
CVE-2022-22717	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	7.0
CVE-2022-22718	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	7.8
CVE-2022-21926	Vulnerabilidad de ejecución remota de código en las extensiones de vídeo HEVC	Importante	7.8
CVE-2022-21927	Vulnerabilidad de ejecución remota de código en las extensiones de vídeo HEVC	Importante	7.8
CVE-2022-21957	Vulnerabilidad de ejecución remota de código en Microsoft Dynamics 365 (local)	Importante	7.2
CVE-2022-21965	Vulnerabilidad de denegación de servicio en Microsoft Teams	Importante	7.5
CVE-2022-22709	Vulnerabilidad de ejecución remota de código en las extensiones de vídeo VP9	Importante	7.8
CVE-2022-22710	Vulnerabilidad de denegación de servicio en el controlador del sistema de archivos de registro común de Windows	Importante	5.5

CVE-2022-22712	Vulnerabilidad de denegación de servicio en Windows Hyper-V	Importante	5.6
CVE-2022-21987	Vulnerabilidad de suplantación de identidad en Microsoft SharePoint Server	Importante	8.0
CVE-2022-21988	Vulnerabilidad de ejecución remota de código en Microsoft Office Visio	Importante	7.8
CVE-2022-23254	Vulnerabilidad de elevación de privilegios en Microsoft Power BI	Importante	4.9
CVE-2022-23269	Vulnerabilidad de suplantación de identidad de Microsoft Dynamics GP	Importante	6.9
CVE-2022-23271	Vulnerabilidad de elevación de privilegios en Microsoft Dynamics GP	Importante	6.5
CVE-2022-21981	Vulnerabilidad de elevación de privilegios en el controlador del sistema de archivos de registro común de Windows	Importante	7.8
CVE-2022-23272	Vulnerabilidad de elevación de privilegios en Microsoft Dynamics GP	Importante	8.1
CVE-2022-23273	Vulnerabilidad de elevación de privilegios en Microsoft Dynamics GP	Importante	7.1
CVE-2022-23274	Vulnerabilidad de ejecución remota de código en Microsoft Dynamics GP	Importante	8.3
CVE-2022-23276	Vulnerabilidad de elevación de privilegios en contenedores de SQL Server para Linux	Importante	7.8
CVE-2022-21968	Característica de seguridad de Microsoft SharePoint Server BypassVulnerability	Importante	4.3

CVE-2022-22715	Vulnerabilidad de elevación de privilegios en el sistema de archivos de canalización con nombre	Importante	7.8
CVE-2022-22716	Vulnerabilidad de divulgación de información en Microsoft Excel	Importante	5.5
CVE-2022-21844	Vulnerabilidad de ejecución remota de código en las extensiones de vídeo HEVC	Importante	7.8
CVE-2022-21974	Vulnerabilidad de ejecución remota de código en Roaming Security Rights Management Services	Importante	7.8
CVE-2022-23261	Vulnerabilidad de manipulación en Microsoft Edge (basada en Chromium)	Moderada	5.3
CVE-2022-0452	Chromium: Uso después de gratis en Navegación Segura	Sin valor asignado	5.3
CVE-2022-0468	Chromium: Uso después de gratis en Pagos	Sin valor asignado	5.3
CVE-2022-0467	Chromium: Implementación inadecuada en el bloqueo de puntero	Sin valor asignado	5.3
CVE-2022-0466	Chromium: Implementación inapropiada en la plataforma de extensiones	Sin valor asignado	5.3
CVE-2022-0465	Chromium: Uso después de la liberación en Extensiones	Sin valor asignado	5.3
CVE-2022-0464	Chromium: Uso después gratis en Accesibilidad	Sin valor asignado	5.3
CVE-2022-0463	Chromium: Uso después gratis en Accesibilidad	Sin valor asignado	5.3
CVE-2022-0462	Chromium: Implementación inapropiada en Scroll	Sin valor asignado	5.3
CVE-2022-0469	Chromium: Uso después de la liberación en Cast	Sin valor asignado	5.3

CVE-2022-0461	Chromium: Derivación de políticas en COOP	Sin valor asignado	5.3
CVE-2022-0459	Chromium: Usar después de gratis en Captura de pantalla	Sin valor asignado	5.3
CVE-2022-0458	Chromium: Usar después de gratis en Thumbnail Tab Strip	Sin valor asignado	5.3
CVE-2022-0457	Chromium: Confusión de tipos en V8	Sin valor asignado	5.3
CVE-2022-0456	Chromium: Uso después de gratis en Web Search	Sin valor asignado	5.3
CVE-2022-0455	Chromium: Implementación inapropiada en modo de pantalla completa	Sin valor asignado	5.3
CVE-2022-0454	Chromium: Desbordamiento del búfer de montón en ANGLE	Sin valor asignado	5.3
CVE-2022-0453	Chromium: Usar después de la liberación en modo lector	Sin valor asignado	5.3
CVE-2022-0460	Chromium: Usar después de liberar en el cuadro de diálogo de ventana	Sin valor asignado	5.3
CVE-2022-0470	Chromium: Acceso a memoria fuera de los límites en V8	Sin valor asignado	5.3

4. MITIGACIÓN / SOLUCIÓN

Para solucionar las vulnerabilidades, Microsoft ha publicado las actualizaciones de seguridad pertinentes. Se recomienda revisar las notas sobre la publicación de este mes y la guía de actualización.

5. REFERENCIAS ADICIONALES

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

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?