Actualización de seguridad de Microsoft - mayo 2022

BCSC-ACTUALIZACION-MICROSOFT-2022-MAYO

TLP:WHITE

www.basquecybersecurity.eus

Mayo 2022

TABLA DE CONTENIDO

Sobre el BCSC 3
1. Resumen ejecutivo 4
2. Recursos afectados 5
3. Análisis técnico 7
4. Mitigación / Solución 20
5. Referencias Adicionales 21

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 mayo de 2022. Con estas actualizaciones se corrigen 75 vulnerabilidades, siendo 8 categorizadas como críticas, 66 como importantes y 1 con severidad baja. Estas vulnerabilidades afectan a productos como Microsoft Office, Microsoft Office Excel, Remote Desktop Client, Windows Remote Desktop, Visual Studio, Windows Server Service o Windows Kernel entre otros.

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

- 1 vulnerabilidad de suplantación (spoofing).
- 6 vulnerabilidades de denegación de servicio.
- 17 vulnerabilidades de divulgación de información.
- 24 vulnerabilidades de ejecución remota de código.
- 21 vulnerabilidades de elevación de privilegios.
- 4 vulnerabilidades de bypass.
- 1 vulnerabilidad que afecta a Magnitude Simba Amazon Redshift ODBC Driver.
- 1 vulnerabilidad que afecta a Azure Data Factory y Azure Synapse Pipelines.

Desde el BCSC recomendamos la aplicación de las actualizaciones para corregirlas.

2. RECURSOS AFECTADOS

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

- .NET and Visual Studio
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Local Security Authority Server (lsasrv)
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Windows ALPC
- Remote Desktop Client
- Role: Windows Fax Service
- Role: Windows Hyper-V
- Self-hosted Integration Runtime
- Tablet Windows User Interface
- Visual Studio
- Visual Studio Code
- Windows Active Directory
- Windows Address Book
- Windows Authentication Methods
- Windows BitLocker
- Windows Cluster Shared Volume (CSV)
- Windows Failover Cluster Automation Server
- Windows Kerberos
- Windows Kernel
- Windows LDAP - Lightweight Directory Access Protocol
- Windows Media
- Windows Network File System
- Windows NTFS
- Windows Point-to-Point Tunneling Protocol
- Windows Print Spooler Components

- Windows Push Notifications
- Windows Remote Access Connection Manager
- Windows Remote Desktop
- Windows Remote Procedure Call Runtime
- Windows Server Service
- Windows Storage Spaces Controller
- Windows WLAN Auto Config Service

3. ANÁLISIS TÉCNICO

Los detalles de las vulnerabilidades críticas corregidas son:

- CVE-2022-26937: Vulnerabilidad de ejecución remota de código del sistema de archivos de red de Windows. Tiene un vector de ataque a nivel de red, con una complejidad de ataque baja. Los privilegios requeridos para un ataque no necesitan que el agente malicioso esté autorizado antes de iniciarlo y, por lo tanto, no requiere ningún acceso a la configuración o los archivos para llevarlo a cabo.
- CVE-2022-22017: Vulnerabilidad de ejecución remota de código del cliente de escritorio remoto. El vector de ataque a nivel de red, con una complejidad de ataque baja. No requiere privilegios para su explotación, por tanto, el agente malicioso no necesita estar autorizado antes de iniciarlo y no requiere ningún acceso a la configuración o los archivos para llevarlo a cabo.
- CVE-2022-29972: Es una vulnerabilidad de inyección de argumentos en el componente de autenticación en el navegador del controlador ODBC Magnitude Simba Amazon Redshift en las versiones que van desde la 1.4.14 a la 1.4.21.1001, desde la 1.4.22 a la 1.4.x, y las anteriores a la 1.4.52, de forma que puede permitir que un usuario local ejecute código arbitrario. Remarcar que esta vulnerabilidad **ha sido divulgada públicamente** y que, para ser explotada, hace falta que el atacante tenga uno de estos roles: Administrador de Synapse, colaborador de Synapse, operador de cómputo Synapse.
- CVE-2022-26923: Vulnerabilidad de elevación de privilegios de los servicios de dominio de Active Directory. Tiene un vector de ataque a nivel de red y una complejidad de explotación baja. En cuanto a los privilegios para llevar a cabo un ataque, el agente malicioso requiere privilegios que otorguen capacidades básicas de usuario que normalmente podrían afectar solo a la configuración y los archivos que pertenecen a un usuario.
- CVE-2022-21972: Vulnerabilidad de ejecución remota de código del protocolo de tunelización punto a punto, con un vector de ataque a nivel de red, una complejidad de explotación alta y sin privilegios requeridos para intentar la explotación del componente vulnerable.
- CVE-2022-23270: Vulnerabilidad de ejecución remota de código del protocolo de tunelización punto a punto, con un vector de ataque a nivel de red y con una complejidad de ataque alta. Los privilegios necesarios para un ataque no requieren que el atacante esté autorizado antes de iniciarlo y, por lo tanto, no requiere ningún acceso a la configuración o los archivos para llevarlo a cabo.
- CVE-2022-26931: Vulnerabilidad de elevación de privilegios de Windows Kerberos, el vector de ataque es a nivel de red con una complejidad de ataque baja. Los privilegios requeridos para un ataque son bajos, lo que implica que no requieren que el agente malicioso esté autorizado antes

de iniciarlo y, por lo tanto, no requiere ningún acceso a la configuración o los archivos para llevarlo a cabo.

- ADV220001: Este identificador está relacionado con la actualización de seguridad CVE-2022-29972 referida anteriormente. Hace referencia a una vulnerabilidad que afecta a Azure Data Factory y Azure Synapse Pipelines. El problema se encontró en el conector de datos ODBC de terceros utilizado para conectarse a Amazon Redshift, en Integration Runtime (IR) en Azure Synapse Pipelines y Azure Data Factory, de forma que podría permitir que un atacante ejecutara comandos remotos en Integration Runtimes.

Fuera de las vulnerabilidades críticas corregidas en esta ocasión, las de mayor relevancia son:

- CVE-2022-26925**:** Vulnerabilidad de falsificación de Windows LSA **que ha sido divulgada de forma pública y está siendo explotada.**
- CVE-2022-22713: Vulnerabilidad de denegación de servicio de Windows Hyper-V, que **ha sido divulgada públicamente**.

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

CVE	Descripción	Severidad	Divulgado	Explotado	CVSS
CVE-2022-26937	Vulnerabilidad de ejecución remota de código en el sistema de archivos de red de Windows	**Crítica**	No	No	9.8
CVE-2022-22017	Vulnerabilidad de ejecución remota de código en el cliente de Escritorio remoto	**Crítica**	No	No	8.8
CVE-2022-29972	Software Insight: CVE-2022-29972 Magnitude Simba Amazon Redshift ODBC Driver	**Crítica**	Sí	No	8.8

CVE-2022-26923	Vulnerabilidad de elevación de privilegios en los Servicios de dominio de Active Directory	**Crítica**	No	No	8.8
CVE-2022-21972	Vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a punto	**Crítica**	No	No	8.1
CVE-2022-23270	Vulnerabilidad de ejecución remota de código en el protocolo de túnel punto a punto	**Crítica**	No	No	8.1
CVE-2022-26931	Vulnerabilidad de elevación de privilegios en Kerberos de Windows	**Crítica**	No	No	7.5
ADV220001	Próximas mejoras en la infraestructura de Azure Data Factory y Azure Synapse Pipeline en respuesta a CVE-2022-29972	**Crítica**	No	No	7.0
CVE-2022-22012	Vulnerabilidad de ejecución remota de código LDAP en Windows	Importante	No	No	9.8
CVE-2022-29130	Vulnerabilidad de ejecución remota de	Importante	No	No	9.8

	código LDAP en Windows				
CVE-2022-26927	Vulnerabilidad de ejecución remota de código en el componente de gráficos de Windows	Importante	No	No	8.8
CVE-2022-22013	Vulnerabilidad de ejecución remota de código LDAP en Windows	Importante	No	No	8.8
CVE-2022-22014	Vulnerabilidad de ejecución remota de código LDAP en Windows	Importante	No	No	8.8
CVE-2022-29108	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	Importante	No	No	8.8
CVE-2022-29128	Vulnerabilidad de ejecución remota de código LDAP en Windows	Importante	No	No	8.8
CVE-2022-29129	Vulnerabilidad de ejecución remota de código LDAP en Windows	Importante	No	No	8.8
CVE-2022-29131	Vulnerabilidad de ejecución remota de código LDAP en Windows	Importante	No	No	8.8

CVE-2022-29133	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	8.8
CVE-2022-29137	Vulnerabilidad de ejecución remota de código LDAP en Windows	Importante	No	No	8.8
CVE-2022-29139	Vulnerabilidad de ejecución remota de código LDAP en Windows	Importante	No	No	8.8
CVE-2022-29141	Vulnerabilidad de ejecución remota de código LDAP en Windows	Importante	No	No	8.8
CVE-2022-22019	Vulnerabilidad de ejecución remota de código en tiempo de ejecución de llamadas a procedimientos remotos	Importante	No	No	8.8
CVE-2022-30129	Vulnerabilidad de ejecución remota de código en Visual Studio Code	Importante	No	No	8.8
CVE-2022-21978	Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server	Importante	No	No	8.2

CVE-2022-26932	Vulnerabilidad de elevación directa de privilegios en espacios de almacenamiento	Importante	No	No	8.2
CVE-2022-26925	Vulnerabilidad de suplantación de identidad de Windows LSA	Importante	Sí	Sí	8.1
CVE-2022-26926	Vulnerabilidad de ejecución remota de código en la Libreta de direcciones de Windows	Importante	No	No	7.8
CVE-2022-29103	Vulnerabilidad de elevación de privilegios en el Administrador de conexiones de acceso remoto de Windows	Importante	No	No	7.8
CVE-2022-29104	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	No	No	7.8
CVE-2022-29105	Vulnerabilidad de ejecución remota de código en Microsoft Windows Media Foundation	Importante	No	No	7.8
CVE-2022-29109	Vulnerabilidad de ejecución remota de código en Microsoft Excel	Importante	No	No	7.8

CVE-2022-29110	Vulnerabilidad de ejecución remota de código en Microsoft Excel	Importante	No	No	7.8
CVE-2022-29113	Vulnerabilidad de elevación de privilegios en Windows Digital Media Receiver	Importante	No	No	7.8
CVE-2022-29115	Vulnerabilidad de ejecución remota de código en el servicio de fax de Windows	Importante	No	No	7.8
CVE-2022-29132	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	No	No	7.8
CVE-2022-29148	Vulnerabilidad de ejecución remota de código en Visual Studio	Importante	No	No	7.8
CVE-2022-23267	Vulnerabilidad de denegación de servicio en .NET y Visual Studio	Importante	No	No	7.5
CVE-2022-29117	Vulnerabilidad de denegación de servicio en .NET y Visual Studio	Importante	No	No	7.5
CVE-2022-29145	Vulnerabilidad de denegación de servicio en .NET y Visual Studio	Importante	No	No	7.5

CVE-2022-26913	Vulnerabilidad de omisión de la característica de seguridad de autenticación de Windows	Importante	No	No	7.4
CVE-2022-26938	Vulnerabilidad de elevación directa de privilegios en espacios de almacenamiento	Importante	No	No	7.0
CVE-2022-26939	Vulnerabilidad de elevación directa de privilegios en espacios de almacenamiento	Importante	No	No	7.0
CVE-2022-22016	Vulnerabilidad de elevación de privilegios en Windows PlayToManager	Importante	No	No	7.0
CVE-2022-29106	Vulnerabilidad de elevación de privilegios en el disco virtual compartido de Windows Hyper-V	Importante	No	No	7.0
CVE-2022-29125	Vulnerabilidad de elevación de privilegios en aplicaciones de notificaciones push de Windows	Importante	No	No	7.0
CVE-2022-29126	Vulnerabilidad de elevación de privilegios en el núcleo de aplicación de la interfaz de	Importante	No	No	7.0

	usuario de Tablet Windows				
CVE-2022-29135	Vulnerabilidad de elevación de privilegios en el volumen compartido de clúster (CSV) de Windows	Importante	No	No	7.0
CVE-2022-29138	Vulnerabilidad de elevación de privilegios en el volumen compartido en clúster de Windows	Importante	No	No	7.0
CVE-2022-29142	Vulnerabilidad de elevación de privilegios en el Kernel de Windows	Importante	No	No	7.0
CVE-2022-23279	Vulnerabilidad de elevación de privilegios en Windows ALPC	Importante	No	No	7.0
CVE-2022-29150	Vulnerabilidad de elevación de privilegios en el volumen compartido de clúster (CSV) de Windows	Importante	No	No	7.0
CVE-2022-29151	Vulnerabilidad de elevación de privilegios en el volumen compartido de clúster (CSV) de Windows	Importante	No	No	7.0
CVE-2022-26934	Vulnerabilidad de divulgación de información de	Importante	No	No	6.5

	componentes de gráficos de Windows				
CVE-2022-26935	Vulnerabilidad de divulgación de información en el servicio de configuración automática de WLAN de Windows	Importante	No	No	6.5
CVE-2022-26936	Vulnerabilidad de divulgación de información de servicio en Windows Server	Importante	No	No	6.5
CVE-2022-26940	Vulnerabilidad de divulgación de información de cliente en el protocolo de Escritorio remoto	Importante	No	No	6.5
CVE-2022-22015	Vulnerabilidad de divulgación de información en el Protocolo de escritorio remoto (RDP) de Windows	Importante	No	No	6.5
CVE-2022-29112	Vulnerabilidad de divulgación de información de componentes de gráficos de Windows	Importante	No	No	6.5
CVE-2022-29134	Vulnerabilidad de divulgación de información de volumen compartido en	Importante	No	No	6.5

	clúster de Windows				
CVE-2022-29120	Vulnerabilidad de divulgación de información de volumen compartido en clúster de Windows	Importante	No	No	6.5
CVE-2022-29121	Vulnerabilidad de denegación de servicio en el servicio de configuración automática de WLAN de Windows	Importante	No	No	6.5
CVE-2022-29122	Vulnerabilidad de divulgación de información de volumen compartido en clúster de Windows	Importante	No	No	6.5
CVE-2022-29123	Vulnerabilidad de divulgación de información de volumen compartido en clúster de Windows	Importante	No	No	6.5
CVE-2022-22713	Vulnerabilidad de denegación de servicio en Windows Hyper-V	Importante	Sí	No	5.6
CVE-2022-26930	Vulnerabilidad de divulgación de información en el Administrador de conexiones de acceso	Importante	No	No	5.5

	remoto de Windows				
CVE-2022-26933	Vulnerabilidad de divulgación de información en Windows NTFS	Importante	No	No	5.5
CVE-2022-22011	Vulnerabilidad de divulgación de información de componentes de gráficos de Windows	Importante	No	No	5.5
CVE-2022-29102	Vulnerabilidad de divulgación de información de clúster de conmutación por error de Windows	Importante	No	No	5.5
CVE-2022-29107	Vulnerabilidad de omisión de la característica de seguridad de Microsoft Office	Importante	No	No	5.5
CVE-2022-29114	Vulnerabilidad de divulgación de información en la cola de impresión de Windows	Importante	No	No	5.5
CVE-2022-29140	Vulnerabilidad de divulgación de información en la cola de impresión de Windows	Importante	No	No	5.5
CVE-2022-29116	Vulnerabilidad de divulgación de información	Importante	No	No	4.7

	en el Kernel de Windows				
CVE-2022-29127	Vulnerabilidad de omisión de la característica de seguridad de BitLocker	Importante	No	No	4.2
CVE-2022-24466	Vulnerabilidad de omisión de la característica de seguridad de Hyper-V en Windows	Importante	No	No	4.1
CVE-2022-30130	Vulnerabilidad de denegación de servicio en .NET Framework	Baja	No	No	3.3

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

- May 2022 Security Updates
- Security Update Guide - Microsoft
- Zero Day initiative-The May 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?