Ok,

Boletín de Seguridad de Microsoft febrero 2021

BCSC_Alerta_Boletín_Seguridad_Microsoft_febrero_2021

TLP:WHITE

www.basquecybersecurity.eus

Febrero 2021

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:

RESUMEN EJECUTIVO

Microsoft ha publicado el boletín mensual de parches de seguridad para el mes de febrero de 2021, conocido como “Patch Tuesday”.

Este mes se han publicado correcciones para 56 vulnerabilidades que afectan a productos tales como Windows Wim32K, Microsoft Exchange Server, Visual Studio, Windows Defender, Windows, TCP/IP, aplicaciones de la suite Office (Excel, Power Point, SharePoint, Outlook), el navegador Edge, etc.

Se trata de 11 vulnerabilidades críticas, 2 moderadas y 43 clasificadas como importantes. Entre todas ellas se ha reportado una vulnerabilidad Zero Day que ha sido activamente explotada y afecta a Windows Win32k.

Además, en este Patch Tuesday se solucionan 6 vulnerabilidades que habían sido descubiertas y publicadas previamente

Todas ellas se solucionan con la aplicación del parche de seguridad asociado a la publicación de este mes de febrero.

ANÁLISIS TÉCNICO

De entre las vulnerabilidades reportadas por Microsoft en este Patch Tuesday de febrero de 2021 se ha publicado un Zero Day, descubierto por investigadores de DBAPPSecurity Co. LTD, que ha sido activamente explotado.

Identificada como "**CVE-2021-1732 – Elevación de privilegios en Windows Win32K",** esta vulnerabilidad permite a un atacante o programa malicioso elevar sus privilegios de usuario para lograr permisos de administrador.

El kernel de algunas versiones de los principales SO de Microsoft (Windows 10 20H2, Windows 10 2004, Windows 10 1909, Windows 10 1809, Windows Server 2019, Windows Server 20H2) se encuentran afectados por esta vulnerabilidad. Por este motivo, desde Microsoft recomiendan a usuarios y administradores de sistemas a aplicar el parche para su corrección.

Junto a esta vulnerabilidad Zero-Day, Microsoft parchea en esta edición de febrero varias vulnerabilidades que han sido publicadas previamente:

- CVE-2021-1721 – Denegación de servicio en .NET Core y Visual Studio.
- CVE-2021-1727 – Elevación de privilegios en Windows Installer
- CVE-2021-1733 – Elevación de privilegios en Sysinternals PsExec
- CVE-2021-24098 – Denegación de servicio en Windows Console Driver
- CVE-2021-24106 – Revelación de información en Windows DirectX
- CVE-2021-26701 – Ejecución de Código remoto en .NET Core

La lista de todas las vulnerabilidades identificadas se detalla a continuación:

Vulnerabilidades Críticas

- CVE-2021-26701 Vulnerabilidad de ejecución de código remoto en .NET Core
- CVE-2021-24112 Vulnerabilidad de ejecución de código remoto en .NET Core
- CVE-2021-24093 Vulnerabilidad de ejecución de código remoto en Windows Graphics Component
- CVE-2021-24081 Vulnerabilidad de ejecución de código remoto en Microsoft Windows Codecs Library
- CVE-2021-24091 Vulnerabilidad de ejecución de código remoto en Windows Camera Codec Pack
- CVE-2021-24078 Vulnerabilidad de ejecución de código remoto en Windows DNS Server
- CVE-2021-24077 Vulnerabilidad de ejecución de código remoto en Windows Fax Service

- CVE-2021-1722 Vulnerabilidad de ejecución de código remoto en Windows Fax Service
- CVE-2021-24088 Vulnerabilidad de ejecución de código remoto en Windows Local Spooler
- CVE-2021-24074 Vulnerabilidad de ejecución de código remoto en Windows TCP/IP
- CVE-2021-24094 Vulnerabilidad de ejecución de código remoto en Windows TCP/IP

Vulnerabilidades Moderadas

- CVE-2021-24109 Vulnerabilidad de elevación de privilegios en Microsoft Azure Kubernetes Service
- CVE-2021-24080 Vulnerabilidad de denegación de servicios en Windows Trust Verification API

Vulnerabilidades Importantes:

- CVE-2021-1721 Vulnerabilidad de denegación de servicio en .NET Core and Visual Studio
- CVE-2021-24111 Vulnerabilidad de denegación de servicio en .NET Framework
- CVE-2021-24087 Vulnerabilidad de elevación de privilegios en Azure IoT CLI extension
- CVE-2021-24105 Vulnerabilidad de ejecución de código remoto en Package Managers Configurations
- CVE-2021-24101 Vulnerabilidad de revelación de información en Microsoft Dataverse
- CVE-2021-1724 Vulnerabilidad de Cross-site scripting en Microsoft Dynamics Business Central
- CVE-2021-24100 Vulnerabilidad de revelación de información en Microsoft Edge para Android
- CVE-2021-24085 Vulnerabilidad de spoofing en Microsoft Exchange Server
- CVE-2021-1730 Vulnerabilidad de spoofing en Microsoft Exchange Server
- CVE-2021-24067 Vulnerabilidad de ejecución de código remoto en Microsoft Excel
- CVE-2021-24068 Vulnerabilidad de ejecución de código remoto en Microsoft Excel

- CVE-2021-24069 Vulnerabilidad de ejecución de código remoto en Microsoft Excel
- CVE-2021-24070 Vulnerabilidad de ejecución de código remoto en Microsoft Excel
- CVE-2021-24071 Vulnerabilidad de revelación de información en Microsoft SharePoint
- CVE-2021-1726 Vulnerabilidad de spoofing en Microsoft SharePoint
- CVE-2021-24066 Vulnerabilidad de ejecución de código remoto en Microsoft SharePoint
- CVE-2021-24072 Vulnerabilidad de ejecución de código remoto en Microsoft SharePoint
- CVE-2021-24114 Vulnerabilidad de revelación de información en Microsoft Teams iOS
- CVE-2021-24076 Vulnerabilidad de revelación de información en Microsoft Windows VMSwitch
- CVE-2021-24073 Vulnerabilidad de spoofing en Skype for Business y Lync
- CVE-2021-24099 Vulnerabilidad de denegación de servicio en Skype for Business y Lync
- CVE-2021-1733 Vulnerabilidad de elevación de privilegios en Sysinternals PsExec y
- CVE-2021-1728 Vulnerabilidad de elevación de privilegios System Center Operations Manager
- CVE-2021-1639 Vulnerabilidad de ejecución de código remoto en Visual Studio Code
- CVE-2021-26700 Vulnerabilidad de ejecución de código remoto en Visual Studio Code npm-script Extension
- CVE-2021-24083 Vulnerabilidad de ejecución de código remoto en Windows Address Book
- CVE-2021-24079 Vulnerabilidad de revelación de información en Windows Backup Engine
- CVE-2021-24098 Vulnerabilidad de denegación de servicio en Windows Console Driver
- CVE-2021-24092 Vulnerabilidad de elevación de privilegios en Microsoft Defender
- CVE-2021-24106 Vulnerabilidad de revelación de información en Windows DirectX

- CVE-2021-24102 Vulnerabilidad de revelación de información en Windows Event Tracing
- CVE-2021-24103 Vulnerabilidad de revelación de información en Windows Event Tracing
- CVE-2021-1727 Vulnerabilidad de revelación de información en Windows Installer Ele
- CVE-2021-24096 Vulnerabilidad de revelación de información en Windows Kernel
- CVE-2021-1732 Vulnerabilidad de revelación de información en Windows Win32k
- CVE-2021-1698 Vulnerabilidad de revelación de información en Windows Win32k
- CVE-2021-24084 Vulnerabilidad de revelación de información en Windows Mobile Device Management
- CVE-2021-24075 Vulnerabilidad de denegación de servicio en Windows Network File System
- CVE-2021-1731 Vulnerabilidad de bypass de herramientas de seguridad en PFX Encryption
- CVE-2021-25195 Vulnerabilidad de elevación de privilegios en Windows PKU2U E
- CVE-2021-24082 Vulnerabilidad de bypass de herramietnas de seguridad en Microsoft.PowerShell.Utility Module WDAC
- CVE-2021-1734 Vulnerabilidad de revelación de información en Windows Remote Procedure Call
- CVE-2021-24086 Vulnerabilidad de denegación de servicios en Windows TCP/IP

Recursos afectados

Los parches de seguridad del mes de febrero de 2021 están asociados a vulnerabilidades de seguridad que afectan a los siguientes productos:

- .NET Core
- .NET Core & Visual Studio
- .NET Framework
- Azure IoT
- Developer Tools
- Microsoft Azure Kubernetes Service
- Microsoft Dynamics
- Microsoft Edge for Android
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Teams
- Microsoft Windows Codecs Library
- Role: DNS Server
- Role: Hyper-V
- Role: Windows Fax Service
- Skype for Business
- SysInternals
- System Center
- Visual Studio
- Visual Studio Code
- Windows Address Book
- Windows Backup Engine
- Windows Console Driver
- Windows Defender
- Windows DirectX
- Windows Event Tracing
- Windows Installer
- Windows Kernel

- Windows Mobile Device Management
- Windows Network File System
- Windows PFX Encryption
- Windows PKU2U
- Windows PowerShell
- Windows Print Spooler Components
- Windows Remote Procedure Call
- Windows TCP/IP
- Windows Trust Verification API

MITIGACIÓN / SOLUCIÓN

Para la mitigación y el parcheo de todas las vulnerabilidades incluidas en el Patch Tuesday de febrero de 2021, Microsoft publica las actualizaciones de seguridad pertinentes junto con sus release notes, las cuales están disponibles en Security Update Guide.

REFERENCIAS ADICIONALES

- Microsoft Security Update Guide
- February 2021 Security Updates
- Microsoft February 2021 Patch Tuesday fixes 56 flaws, 1 zero-day

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?