Boletín de Seguridad de Microsoft enero 2021

BCSC_Alerta_Boletín_Seguridad_Microsoft_enero_2021

TLP:WHITE

www.basquecybersecurity.eus

Enero 2021

TABLA DE CONTENIDO

Sobre el BCSC 3
Resumen ejecutivo 4
Análisis técnico 5
Recursos afectados 10
Mitigación / Solución 11
Referencias Adicionales 12

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 enero de 2021, conocido como “Patch Tuesday”.

Este mes se han publicado correcciones para 83 vulnerabilidades que afectan a productos tales como Microsoft Defender, Visual Studio, Hyper-V, WalletService, aplicaciones de la suite Office (Excel, Power Point, SharePoint, Outlook), el navegador Edge, etc.

Se trata de 10 vulnerabilidades críticas y 73 clasificadas como importantes. Entre todas ellas se ha reportado una vulnerabilidad Zero Day con evidencias de haber sido explotada que afecta a Microsoft Defender así como una vulnerabilidad hecha pública el pasado diciembre en el servicio Windows splwow64, que no habría sido explotada según las informaciones de Microsoft.

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

ANÁLISIS TÉCNICO

De entre las vulnerabilidades reportadas por Microsoft en este Patch Tuesday de enero de 2021 se ha detectado una Zero Day que se estima que ha sido explotado previamente a la publicación y solución del misma.

La vulnerabilidad, con código **CVE-2021-1647,** permite la ejecución de código remoto en el software de seguridad Microsoft Defender y afecta hasta la versión 1.1.17600.5 del Microsoft Malware Protection Engine. Se ha aplicado la solución en la versión 1.1.17700.4 y superiores que ya no son vulnerables.

Desde Microsoft, instan a los usuarios y administradores de sistemas a verificar que la última versión de las actualizaciones está descargada e instalada. Se trata de actualizaciones que el Microsoft Malware Protection Engine realiza de manera periódica y automática sin necesidad de ninguna acción por parte del usuario. No obstante, se pueden forzar manualmente.

Por otro lado, en el boletín, también se corrige una vulnerabilidad que hizo pública Trend Micro`s Zero Day Initiative el pasado 15 de diciembre de 2020 y que, según la información de Microsoft, no habría sido explotada. Esta vulnerabilidad, con código **CVE-2021-1648**, puede ser utilizada para la elevación de privilegios ante un ataque en el servicio Windows splwow64.

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

Vulnerabilidades Críticas

- CVE-2021-1668 Vulnerabilidad de ejecución de código remoto en Microsoft DTV-DVD Video Decoder
- CVE-2021-1705 Vulnerabilidad de corrupción de memoria en Microsoft Edge (HTML-based
- CVE-2021-1665 Vulnerabilidad de ejecución de código remoto en GDI+
- CVE-2021-1647 Vulnerabilidad de ejecución de código remoto en Microsoft Defender
- CVE-2021-1643 Vulnerabilidad de ejecución de código remoto en HEVC Video Extensions
- CVE-2021-1666 Vulnerabilidad de ejecución de código remoto en Remote Procedure Call Runtime
- CVE-2021-1673 Vulnerabilidad de ejecución de código remoto en Remote Procedure Call Runtime
- CVE-2021-1658 Vulnerabilidad de ejecución de código remoto en Remote Procedure Call Runtime
- CVE-2021-1667 Vulnerabilidad de ejecución de código remoto en Remote Procedure Call Runtime

- CVE-2021-1660 Vulnerabilidad de ejecución de código remoto en Remote Procedure Call Runtime

Vulnerabilidades Importantes:

- CVE-2021-1725 Vulnerabilidad de exposición de información en Bot Framework SDK
- CVE-2021-1723 Vulnerabilidad de denegación de servicio en ASP.NET Core y Visual Studio
- CVE-2021-1677 Vulnerabilidad de spoofing en Azure Active Directory Pod Identity
- CVE-2021-1683 Vulnerabilidad de bypass en los mecanismos de seguridad de Windows Bluetooth
- CVE-2021-1638 Vulnerabilidad de bypass en los mecanismos de seguridad de Windows Bluetooth
- CVE-2021-1684 Vulnerabilidad de bypass en los mecanismos de seguridad de Windows Bluetooth
- CVE-2021-1709 Vulnerabilidad de elevación de privilegios en Windows Win32k
- CVE-2021-1696 Vulnerabilidad de exposición de información en Windows Graphics Component
- CVE-2021-1708 Vulnerabilidad de exposición de información en Windows GDI+
- CVE-2021-1713 Vulnerabilidad de ejecución de código remoto en Microsoft Excel
- CVE-2021-1714 Vulnerabilidad de ejecución de código remoto en Microsoft Excel
- CVE-2021-1711 Vulnerabilidad de ejecución de código remoto en Microsoft Excel
- CVE-2021-1715 Vulnerabilidad de ejecución de código remoto en Microsoft Excel
- CVE-2021-1716 Vulnerabilidad de ejecución de código remoto en Microsoft Excel
- CVE-2021-1712 Vulnerabilidad de elevación de privilegios en Microsoft SharePoint
- CVE-2021-1707 Vulnerabilidad de ejecución de código remoto en Microsoft SharePoint Server
- CVE-2021-1718 Vulnerabilidad de manipulación en Microsoft SharePoint Server
- CVE-2021-1717 Vulnerabilidad de spoofing en Microsoft SharePoint

- CVE-2021-1719 Vulnerabilidad de elevación de privilegios en Microsoft SharePoint
- CVE-2021-1641 Vulnerabilidad de spoofing en Microsoft SharePoint
- CVE-2021-1702 Vulnerabilidad de elevación de privilegios en Windows Remote Procedure Call Runtime
- CVE-2021-1649 Vulnerabilidad de elevación de privilegios en Active Template Library
- CVE-2021-1676 Vulnerabilidad de exposición de información en Windows NT Lan Manager Datagram Receiver Driver
- CVE-2021-1689 Vulnerabilidad de elevación de privilegios en Windows Multipoint Management
- CVE-2021-1657 Vulnerabilidad de ejecución de código remoto en Windows Fax Compose Form
- CVE-2021-1646 Vulnerabilidad de elevación de privilegios en Windows WLAN Service
- CVE-2021-1650 Vulnerabilidad de elevación de privilegios en Windows Runtime C++ Template Library
- CVE-2021-1706 Vulnerabilidad de elevación de privilegios en Windows LUAFV
- CVE-2021-1699 Vulnerabilidad de exposición de información en Windows (modem.sys)
- CVE-2021-1644 Vulnerabilidad de ejecución de código remoto en HEVC Video Extensions
- CVE-2021-1637 Vulnerabilidad de exposición de información en Windows DNS Query
- CVE-2021-1636 Vulnerabilidad de elevación de privilegios en Microsoft SQL
- CVE-2020-26870 Vulnerabilidad de ejecución de código remoto en Visual Studio
- CVE-2021-1642 Vulnerabilidad de elevación de privilegios en Windows AppX Deployment Extensions
- CVE-2021-1685 Vulnerabilidad de elevación de privilegios en Windows AppX Deployment Extensions
- CVE-2021-1679 Vulnerabilidad de denegación de servicio en Windows CryptoAPI
- CVE-2021-1652 Vulnerabilidad de elevación de privilegios en Windows CSC Service

- CVE-2021-1654 Vulnerabilidad de elevación de privilegios en Windows CSC Service
- CVE-2021-1659 Vulnerabilidad de elevación de privilegios en Windows CSC Service
- CVE-2021-1653 Vulnerabilidad de elevación de privilegios en Windows CSC Service
- CVE-2021-1655 Vulnerabilidad de elevación de privilegios en Windows CSC Service
- CVE-2021-1693 Vulnerabilidad de elevación de privilegios en Windows CSC Service
- CVE-2021-1688 Vulnerabilidad de elevación de privilegios en Windows CSC Service
- CVE-2021-1680 Vulnerabilidad de elevación de privilegios en Diagnostics Hub Standard Collector
- CVE-2021-1651 Vulnerabilidad de elevación de privilegios en Diagnostics Hub Standard Collector
- CVE-2021-1645 Vulnerabilidad de exposición de información en Windows Docker
- CVE-2021-1703 Vulnerabilidad de elevación de privilegios en Windows Event Logging Service
- CVE-2021-1662 Vulnerabilidad de elevación de privilegios en Windows Event Tracing
- CVE-2021-1691 Vulnerabilidad de denegación de servicio en Hyper-V
- CVE-2021-1704 Vulnerabilidad de elevación de privilegios en Hyper-V
- CVE-2021-1692 Vulnerabilidad de denegación de servicio en Hyper-V
- CVE-2021-1661 Vulnerabilidad de elevación de privilegios en Windows Installer
- CVE-2021-1697 Vulnerabilidad de elevación de privilegios en Windows InstallService
- CVE-2021-1682 Vulnerabilidad de elevación de privilegios en Windows Kernel
- CVE-2021-1710 Vulnerabilidad de ejecución de código remoto en Microsoft Windows Media Foundation
- CVE-2021-1678 Vulnerabilidad de bypass en los mecanismos de seguridad de NTLM
- CVE-2021-1695 Vulnerabilidad de elevación de privilegios en Windows Print Spooler

- CVE-2021-1663 Vulnerabilidad de exposición de información en Windows Projected File System FS Filter Driver
- CVE-2021-1672 Vulnerabilidad de exposición de información en Windows Projected File System FS Filter Driver
- CVE-2021-1670 Vulnerabilidad de exposición de información en Windows Projected File System FS Filter Driver
- CVE-2021-1674 Vulnerabilidad de bypass en los mecanismos de seguridad de Windows Remote Desktop Protocol Core
- CVE-2021-1669 Vulnerabilidad de bypass en los mecanismos de seguridad de Windows Remote Desktop
- CVE-2021-1701 Vulnerabilidad de ejecución de código remoto en Remote Procedure Call Runtime
- CVE-2021-1700 Vulnerabilidad de ejecución de código remoto en Remote Procedure Call Runtime
- CVE-2021-1664 Vulnerabilidad de ejecución de código remoto en Remote Procedure Call Runtime
- CVE-2021-1671 Vulnerabilidad de ejecución de código remoto en Remote Procedure Call Runtime
- CVE-2021-1648 Vulnerabilidad de elevación de privilegios en Microsoft splwow64
- CVE-2021-1656 Vulnerabilidad de exposición de información en TPM Device Driver
- CVE-2021-1694 Vulnerabilidad de elevación de privilegios en Windows Update Stack
- CVE-2021-1686 Vulnerabilidad de elevación de privilegios en Windows WalletService
- CVE-2021-1681 Vulnerabilidad de elevación de privilegios en Windows WalletService
- CVE-2021-1690 Vulnerabilidad de elevación de privilegios en Windows WalletService
- CVE-2021-1687 Vulnerabilidad de elevación de privilegios en Windows WalletService

Recursos afectados

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

- Microsoft Windows
- Microsoft Edge (EdgeHTML-based)
- Microsoft Office and Microsoft Office Services and Web Apps
- Microsoft Windows Codecs Library
- Visual Studio
- SQL Server
- Microsoft Malware Protection Engine
- .NET Core
- .NET Repository
- ASP .NET
- Azure

MITIGACIÓN / SOLUCIÓN

Para la mitigación y el parcheo de todas las vulnerabilidades incluidas en el Patch Tuesday de enero 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
- January 2021 Security Updates
- Microsoft patches Defender antivirus zero-day exploited in the wild
- Microsoft January 2021 Patch Tuesday fixes 83 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?