Actualizaciones de Seguridad de Microsoft Diciembre 2020

BCSC-ACTUALIZACION-MICROSOFT_2020_DICIEMBRE

TLP:WHITE

www.basquecybersecurity.eus

Diciembre 2020

TABLA DE CONTENIDO

Sobre el BCSC 3
Resumen ejecutivo 4
Análisis técnico 5
Recursos afectados 9
Mitigación / Solución 10
Referencias Adicionales 11

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 diciembre de 2020, conocido como “Patch Tuesday”.

Este mes se han publicado correcciones para 58 vulnerabilidades que afectan a productos tales como Microsoft Exchange, Hyper-V, Windows NTFS, aplicaciones de la suite Office (Excel, Power Point, SharePoint, Outlook), el navegador Edge, etc.

Se trata de 9 vulnerabilidades críticas, 47 clasificadas como importantes y 2 con criticidad moderada. Entre todas ellas no hay ningún zero-day o vulnerabilidades previamente explotadas.

ANÁLISIS TÉCNICO

No se han detectado vulnerabilidades estén siendo explotadas activamente. No obstante, algunas de las publicadas resultan especialmente relevantes debido al posible impacto que pudiera tener su explotación:

- **CVE-2020-17095 - Hyper-V** - Vulnerabilidad de ejecución de Código remoto: Permite programas maliciosos en una Máquina Virtual Hyper-V para, a su vez, ejecutar código en el Host.
- **CVE-2020-17096 - Windows NTFS** – Vulnerabilidad de ejecución de código remoto: esta vulnerabilidad puede ser explotada en local para elevar privilegios o bien de manera remota, a través de SMBv2, para la ejecución de comandos.
- **CVE-2020-17099 - Windows Lock Screen** – Bypass en los mecanismos de seguridad: Permite a un atacante local la ejecución de comandos desde un dispositivo Windows bloqueado.

Además de los parches para la corrección de vulnerabilidades, Microsoft ha publicado un aviso sobre la vulnerabilidad de envenenamiento de caché DNS conocida como SAD DNS, recientemente descubierta por investigadores de las Universidades de Tsinghua y California. El aviso incluye un workaround para resolver o mitigar esta vulnerabilidad mediante la modificación del registro de Windows, para cambiar el tamaño máximo de paquetes UDP a 1221 bytes. Para solicitudes mayores a este valor, el DNS resolver cambiará a conexiones TCP.

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

Vulnerabilidades Críticas

- CVE-2020-17158 Vulnerabilidad de ejecución de código remoto en Microsoft Dynamics 365 for Finance and Operations
- CVE-2020-17152 Vulnerabilidad de ejecución de código remoto en Microsoft Dynamics 365 for Finance and Operations
- CVE-2020-17131 Vulnerabilidad de corrupción de memoria en Chakra Scripting Engine.
- CVE-2020-17117 Vulnerabilidad de ejecución de código remoto en Microsoft Exchange.
- CVE-2020-17132 Vulnerabilidad de ejecución de código remoto en Microsoft Exchange.
- CVE-2020-17142 Vulnerabilidad de ejecución de código remoto en Microsoft Exchange.
- CVE-2020-17121 Vulnerabilidad de ejecución de código remoto en Microsoft SharePoint.
- CVE-2020-17118 Vulnerabilidad de ejecución de código remoto en Microsoft SharePoint.

- CVE-2020-17095 Vulnerabilidad de ejecución de código remoto en Hyper-V.

Vulnerabilidades Importantes:

- CVE-2020-17145 Vulnerabilidad de Spoofing en Azure DevOps Server and Team Foundation Services.
- CVE-2020-17135 Vulnerabilidad de Spoofing en Azure DevOps Server
- CVE-2020-17002 Bypass en los mecanismos de seguridad de Azure SDK for C.
- CVE-2020-16971 Bypass en los mecanismos de seguridad de Azure SDK for Java Security.
- CVE-2020-17160 Bypass en los mecanismos de seguridad de Azure Sphere Security (Retractada)CVE-2020-17147 Vulnerabilidad a Cross-site scripting en Dynamics CRM Webclient.
- CVE-2020-17133 Vulnerabilidad de Exposición de Información en Microsoft Dynamics Business Central/NAV.
- CVE-2020-17143 Vulnerabilidad de exposición de información en Microsoft Exchange.
- CVE-2020-17144 Vulnerabilidad de ejecución de código remoto en Microsoft Exchange.
- CVE-2020-17141 Vulnerabilidad de ejecución de código remoto en Microsoft Exchange.
- CVE-2020-17137 Vulnerabilidad de elevación de privilegios e DirectX Graphics.
- CVE-2020-17098 Vulnerabilidad de exposición de información en Windows GDI+.
- CVE-2020-17130 Vulnerabilidad de Bypass en los mecanismos de seguridad de Microsoft Excel.
- CVE-2020-17128 Vulnerabilidad de ejecución de código remoto en Microsoft Excel.
- CVE-2020-17129 Vulnerabilidad de ejecución de código remoto en Microsoft Excel.
- CVE-2020-17124 Vulnerabilidad de ejecución de código remoto en Microsoft PowerPoint.
- CVE-2020-17123 Vulnerabilidad de ejecución de código remoto en Microsoft Excel.
- CVE-2020-17119 Vulnerabilidad de ejecución de código remoto en Microsoft Outlook.

- CVE-2020-17125 Vulnerabilidad de ejecución de código remoto en Microsoft Excel.
- CVE-2020-17127 Vulnerabilidad de ejecución de código remoto en Microsoft Excel.
- CVE-2020-17126 Vulnerabilidad de exposición de información en Microsoft Excel.
- CVE-2020-17122 Vulnerabilidad de ejecución de código remoto en Microsoft Excel.
- CVE-2020-17120 Vulnerabilidad de exposición de información en Microsoft SharePoint.
- CVE-2020-17089 Vulnerabilidad de elevación de privilegios en Microsoft SharePoint.
- CVE-2020-17136 Vulnerabilidad de elevación de privilegios en Windows Cloud Files Mini Filter Driver.
- CVE-2020-16996 Vulnerabilidad de Bypass en los mecanismos de seguridad de Kerberos.
- CVE-2020-17138 Vulnerabilidad de exposición de información en Windows Error Reporting.
- CVE-2020-17092 Vulnerabilidad de elevación de privilegios en Windows Network Connections Service.
- CVE-2020-17139 Vulnerabilidad de Bypass en los mecanismos de seguridad de Windows Overlay Filter.
- CVE-2020-17103 Vulnerabilidad de elevación de privilegios en Windows Cloud Files Mini Filter Driver.
- CVE-2020-17134 Vulnerabilidad de elevación de privilegios en Windows Cloud Files Mini Filter Driver.
- CVE-2020-17148 Vulnerabilidad de ejecución de código remoto en Visual Studio Code Remote Development Extension.
- CVE-2020-17159 Vulnerabilidad de ejecución de código remoto en Visual Studio Code Java Extension Pack.
- CVE-2020-17156 Vulnerabilidad de ejecución de código remoto en Visual Studio.
- CVE-2020-17150 Vulnerabilidad de ejecución de código remoto en Visual Studio.
- CVE-2020-16960 Vulnerabilidad de ejecución de código remoto en Windows Backup Engine.
- CVE-2020-16958 Vulnerabilidad de ejecución de código remoto en Windows Backup Engine.

- CVE-2020-16959 Vulnerabilidad de ejecución de código remoto en Windows Backup Engine.
- CVE-2020-16961 Vulnerabilidad de ejecución de código remoto en Windows Backup Engine.
- CVE-2020-16964 Vulnerabilidad de ejecución de código remoto en Windows Backup Engine.
- CVE-2020-16963 Vulnerabilidad de ejecución de código remoto en Windows Backup Engine.
- CVE-2020-16962 Vulnerabilidad de elevación de privilegios en Windows Backup Engine.
- CVE-2020-17094 Vulnerabilidad de exposición de información en Windows Error Reporting.
- CVE-2020-17099 Vulnerabilidad de bypass en los mecanismos de seguridad de Windows Lock Screen.
- CVE-2020-17097 Vulnerabilidad de elevación de privilegios en Windows Digital Media Receiver.
- CVE-2020-17096 Vulnerabilidad de ejecución de código remoto en Windows NTFS
- CVE-2020-17140 Vulnerabilidad de exposición de información en Windows SMB.

Vulnerabilidades moderadas:

- CVE-2020-17153 Vulnerabilidad de spoofing en Microsoft Edge para Android.
- CVE-2020-17115 Vulnerabilidad de spoofing en Microsoft SharePoint.

Recursos afectados

Los parches de seguridad del mes de diciembre de 2020 están asociados a vulnerabilidades de seguridad que afectan a los siguientes productos:

- Azure DevOps
- Azure SDK
- Azure Sphere
- Microsoft Dynamics
- Microsoft Edge
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Windows
- Microsoft Windows DNS
- Visual Studio
- Windows Backup Engine
- Windows Error Reporting
- Windows Hyper-V
- Windows Lock Screen
- Windows Media
- Windows SMB

MITIGACIÓN / SOLUCIÓN

Para la mitigación y el parcheo de todas las vulnerabilidades incluidas en el Patch Tuesday de diciembre de 2020, Microsoft publica las actualizaciones de seguridad pertinentes junto con sus release notes, las cuales están disponibles en Security Update Guide.

REFERENCIAS ADICIONALES

- December 2020 Security Updates
- Información sobre la implementación de la actualización de seguridad: martes, 8 de diciembre de 2020
- Microsoft Security Update Guide
- Microsoft Guidance for Addressing Spoofing Vulnerability in DNS Resolver

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?