# Boletín de Seguridad de Microsoft Noviembre 2020

BCSC_ALERTA_Boletín_Seguridad_Microsoft_Noviembre_2020

TLP:WHITE

Noviembre 2020

# TABLA DE CONTENIDO

Sobre el BCSC ..... 3
Resumen ejecutivo ..... 4
Análisis técnico ..... 5
Recursos afectados ..... 11
Mitigación / Solución ..... 12
Referencias Adicionales ..... 13

## 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 su boletín mensual de parches de seguridad para el mes de noviembre de 2020, conocido como “Patch Tuesday”.

En el boletín de este mes, la compañía corrige 112 errores de seguridad en diversos productos tales como Microsoft Windows, Office, Internet Explorer (IE), Edge, Exchange Server, Azure Sphere, Windows Defender, Microsoft Teams, Visual Studio, etc.

Se trata de 17 vulnerabilidades críticas, 93 clasificadas como importantes y 2 con criticidad baja. Entre todas ellas se ha confirmado que sólo una está siendo explotada activamente con fines maliciosos por lo que se recomienda aplicar los parches de seguridad lo antes posible para corregir dichos fallos.

# ANÁLISIS TÉCNICO

De las 112 vulnerabilidades que han hecho públicas, únicamente una se ha confirmado que está siendo explotada activamente.

La vulnerabilidad, a la cual se le ha asignado el identificador CVE-2020-17087, de acuerdo con la información proporcionada por Microsoft, ha sido explotada sobre usuarios de Windows 7 y Windows 10.

Los atacantes están utilizando una vulnerabilidad en Chrome (CVE-2020-15999, parcheada en la versión 86.0.4240.111) para ejecutar código malicioso en Chrome y, a continuación, mediante el Zero Day de Windows evitar la sandbox de seguridad de Chrome y elevar privilegios sobre el código para atacar el Sistema Operativo.

De acuerdo con la información del Boletín de Microsoft para esta vulnerabilidad, el Zero Day se localiza en el Kernel de Windows e impacta sobre todas las versiones actualmente soportadas de Windows. Esto incluye todas las versiones posteriores después de Windows 7, y todas las distribuciones de Windows Server.

El resto de las vulnerabilidades identificadas son las siguientes:

**Vulnerabilidades Críticas:**

- CVE-2020-17105: Ejecución de código remoto sobre la extensión de video AV1.
- CVE-2020-16988: Vulnerabilidad de Elevación de Privilegios en Azure Sphere.
- CVE-2020-17048: Vulnerabilidad en Chakra de scripting de corrupción de memoria.
- CVE-2020-17101: Vulnerabilidad de ejecución de código remoto en extensiones de imagen HEIF.
- CVE-2020-17106: Vulnerabilidad de ejecución de código remoto en extensiones de imagen HEVC.
- CVE-2020-17107: Vulnerabilidad de ejecución de código remoto en extensiones de imagen HEVC.
- CVE-2020-17108: Vulnerabilidad de ejecución de código remoto en extensiones de imagen HEVC.
- CVE-2020-17109: Vulnerabilidad de ejecución de código remoto en extensiones de imagen HEVC.
- CVE-2020-17110: Vulnerabilidad de ejecución de código remoto en extensiones de imagen HEVC.
- CVE-2020-17053: Vulnerabilidad de corrupción de memoria en Internet Explorer.

- CVE-2020-17058: Vulnerabilidad de corrupción de memoria en explorador de Microsoft.
- CVE-2020-17078: Vulnerabilidad de ejecución de código remoto en Raw Image.
- CVE-2020-17079: Vulnerabilidad de ejecución de código remoto en Raw Image.
- CVE-2020-17082: Vulnerabilidad de ejecución de código remoto en Raw Image.
- CVE-2020-17052: Vulnerabilidad de corrupción de memoria en el motor de Scripting.
- CVE-2020-17051: Vulnerabilidad de ejecución de código remoto en Windows Network File System.
- CVE-2020-17042: Vulnerabilidad de ejecución de código remoto en Windows Print Spooler.

**Vulnerabilidades Importantes:**

- CVE-2020-1325: Vulnerabilidad a Spoofing sobre Azure DevOps server y Team Foundation Services.
- CVE-2020-16986: Vulnerabilidad de denegación de servicio sobre Azure Sphere.
- CVE-2020-16981: Vulnerabilidad de Elevación de Privilegios en Azure Sphere.
- CVE-2020-16989: Vulnerabilidad de Elevación de Privilegios en Azure Sphere.
- CVE-2020-16992: Vulnerabilidad de Elevación de Privilegios en Azure Sphere.
- CVE-2020-16993: Vulnerabilidad de Elevación de Privilegios en Azure Sphere.
- CVE-2020-16985: Vulnerabilidad de revelación de Información en Azure Sphere.
- CVE-2020-16990: Vulnerabilidad de revelación de Información en Azure Sphere.
- CVE-2020-16983: Vulnerabilidad de manipulación den Azure Sphere.
- CVE-2020-16970: Vulnerabilidad de ejecución de código sin firmar Azure Sphere.
- CVE-2020-16982: Vulnerabilidad de ejecución de código sin firmar Azure Sphere.
- CVE-2020-16984: Vulnerabilidad de ejecución de código sin firmar Azure Sphere.

- CVE-2020-16987: Vulnerabilidad de ejecución de código sin firmar Azure Sphere.
- CVE-2020-16991: Vulnerabilidad de ejecución de código sin firmar Azure Sphere.
- CVE-2020-16994: Vulnerabilidad de ejecución de código sin firmar Azure Sphere.
- CVE-2020-17054: Vulnerabilidad en Chakra de scripting de corrupción de memoria.
- CVE-2020-16998: Elevación de privilegios en DirectX.
- CVE-2020-17049: Vulnerabilidad de bypass en Kerberos Security Feature.
- CVE-2020-17090: Bypass de Microsoft Defender para Endpoint Security Feature.
- CVE-2020-17005: Vulnerabilidad de Cross-site Scripting en Microsoft Dynamics 365.
- CVE-2020-17006: Vulnerabilidad de Cross-site Scripting en Microsoft Dynamics 365.
- CVE-2020-17018: Vulnerabilidad de Cross-site Scripting en Microsoft Dynamics 365.
- CVE-2020-17021: Vulnerabilidad de Cross-site Scripting en Microsoft Dynamics 365.
- CVE-2020-17019: Vulnerabilidad de ejecución de código remoto en Microsoft Excel.
- CVE-2020-17064: Vulnerabilidad de ejecución de código remoto en Microsoft Excel.
- CVE-2020-17065: Vulnerabilidad de ejecución de código remoto en Microsoft Excel.
- CVE-2020-17066: Vulnerabilidad de ejecución de código remoto en Microsoft Excel.
- CVE-2020-17067: Bypass de Microsoft Excel Security Feature.
- CVE-2020-17085: Vulnerabilidad de denegación de servicio en servidores Microsoft Exchange.
- CVE-2020-17083: Vulnerabilidad de ejecución de código remoto en servidores Microsoft Exchange.
- CVE-2020-17084: Vulnerabilidad de ejecución de código remoto en servidores Microsoft Exchange.
- CVE-2020-17062: Vulnerabilidad de ejecución de código remoto en Microsoft Office Access Connectivity Engine.

- CVE-2020-17063: Vulnerabilidad a spoofing en Microsoft Office Online.
- CVE-2020-17081: Vulnerabilidad de exposición de información en la extensión Microsoft Raw Image.
- CVE-2020-17086: Vulnerabilidad de exposición de información en la extensión Microsoft Raw Image.
- CVE-2020-16979: Vulnerabilidad de exposición de información en la extensión Microsoft Sharepoint.
- CVE-2020-17017: Vulnerabilidad de exposición de información en la extensión Microsoft Sharepoint.
- CVE-2020-17061: Vulnerabilidad de ejecución de código remoto en Microsoft Sharepoint.
- CVE-2020-17016: Vulnerabilidad a spoofing en Microsoft Sharepoint.
- CVE-2020-17060: Vulnerabilidad a spoofing en Microsoft Sharepoint.
- CVE-2020-17091: Vulnerabilidad de ejecución de código remoto en Microsoft Teams.
- CVE-2020-17020: Vulnerabilidad de bypass en Microsoft Word Security Feature.
- CVE-2020-17000: Vulnerabilidad de exposición de información de Cliente de RDP (Remote Desktop Protocol).
- CVE-2020-16997: Vulnerabilidad de exposición de información de Servidor de RDP (Remote Desktop Protocol).
- CVE-2020-17104: Vulnerabilidad de ejecución de código remoto en la extensión de Visual Studio Code JSHint.
- CVE-2020-17100: Vulnerabilidad de manipulación de Visual Studio.
- CVE-2020-17102: Vulnerabilidad de exposición de información en extensiones WebP Image.
- CVE-2020-17010: Vulnerabilidad de elevación de privilegios en Win32k.
- CVE-2020-17038: Vulnerabilidad de elevación de privilegios en Win32k.
- CVE-2020-17013: Vulnerabilidad de exposición de información en Win32k.
- CVE-2020-17012: Vulnerabilidad de elevación de privilegios en Windows Bind Filter.
- CVE-2020-17113: Vulnerabilidad de exposición de información en Windows Camera Codec.
- CVE-2020-17029: Vulnerabilidad de exposición de información en Windows Canonical Display Driver.

- CVE-2020-17024: Vulnerabilidad de elevación de privilegios en Windows Client Side Rendering Print.
- CVE-2020-17088: Vulnerabilidad de elevación de privilegios en Windows Common Log File System Driver.
- CVE-2020-17071: Vulnerabilidad de exposición de información en Windows Delivery Optimization.
- CVE-2020-17007: Vulnerabilidad de exposición de información en Windows Error Reporting.
- CVE-2020-17036: Vulnerabilidad de exposición de información en Windows Function Discovery.
- CVE-2020-17068: Vulnerabilidad de ejecución de código remoto en Windows GDI+.
- CVE-2020-17004: Vulnerabilidad de exposición de información en Windows Graphics Component.
- CVE-2020-17040: Vulnerabilidad de bypass de funciones de seguridad en Windows Hyper-V.
- CVE-2020-17035: Vulnerabilidad de elevación de privilegios en Windows kernel.
- CVE-2020-17045: Vulnerabilidad de exposición de información en Windows KernelStream.
- CVE-2020-17030: Vulnerabilidad de exposición de información en Windows MSCTF Server.
- CVE-2020-17069: Vulnerabilidad de exposición de información en Windows NDIS.
- CVE-2020-17047: Vulnerabilidad a denegación de servicio en Windows Network File System.
- CVE-2020-17056: Vulnerabilidad de exposición de información en Windows Network File System.
- CVE-2020-17011: Vulnerabilidad de elevación de privilegios en Windows Port Class Library.
- CVE-2020-17041: Vulnerabilidad de elevación de privilegios en Windows Print Configuration.
- CVE-2020-17001: Vulnerabilidad de elevación de privilegios en Windows Print Spooler.
- CVE-2020-17014: Vulnerabilidad de elevación de privilegios en Windows Print Spooler.
- CVE-2020-17025: Vulnerabilidad de elevación de privilegios en Windows Remote Access.

- CVE-2020-17026: Vulnerabilidad de elevación de privilegios en Windows Remote Access.
- CVE-2020-17027: Vulnerabilidad de elevación de privilegios en Windows Remote Access.
- CVE-2020-17028: Vulnerabilidad de elevación de privilegios en Windows Remote Access.
- CVE-2020-17031: Vulnerabilidad de elevación de privilegios en Windows Remote Access.
- CVE-2020-17032: Vulnerabilidad de elevación de privilegios en Windows Remote Access.
- CVE-2020-17033: Vulnerabilidad de elevación de privilegios en Windows Remote Access.
- CVE-2020-17034: Vulnerabilidad de elevación de privilegios en Windows Remote Access.
- CVE-2020-17043: Vulnerabilidad de elevación de privilegios en Windows Remote Access.
- CVE-2020-17044: Vulnerabilidad de elevación de privilegios en Windows Remote Access.
- CVE-2020-17055: Vulnerabilidad de elevación de privilegios en Windows Remote Access.
- CVE-2020-1599: Vulnerabilidad de Spoofing en Windows.
- CVE-2020-17070: Vulnerabilidad de elevación de privilegios en Windows Update Medic Service.
- CVE-2020-17073: Vulnerabilidad de elevación de privilegios en Windows Update Orchestrator Service.
- CVE-2020-17074: Vulnerabilidad de elevación de privilegios en Windows Update Orchestrator Service.
- CVE-2020-17076: Vulnerabilidad de elevación de privilegios en Windows Update Orchestrator Service.
- CVE-2020-17077: Vulnerabilidad de elevación de privilegios en Windows Update Stack.
- CVE-2020-17075: Vulnerabilidad de elevación de privilegios en Windows USO Core Worker.
- CVE-2020-17037: Vulnerabilidad de elevación de privilegios en Windows WalletService.
- CVE-2020-16999: Vulnerabilidad de exposición de información en Windows WalletService.

- CVE-2020-17057: Vulnerabilidad de elevación de privilegios en Windows Win32k.

**Vulnerabilidades con criticidad baja:**

- CVE-2020-17015: Vulnerabilidad a spoofing en Microsoft Sharepoint.
- CVE-2020-17046: Vulnerabilidad de exposición de información en Windows Error Reporting.

## Recursos afectados

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

- Azure Devops
- Azure Sphere
- Microsoft Windows Codecs Library
- Visual Studio
- Microsoft Teams
- Windows Defender
- Common Log File System Driver
- Windows Kernel
- Microsoft Exchange Server
- Windows Update Stack
- Windows NDIS
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Browsers
- Microsoft Windows
- Microsoft Scripting Engine
- Windows WalletService
- Microsoft Dynamics

## MITIGACIÓN / SOLUCIÓN

Para la mitigación y el parcheo de todas las vulnerabilidades incluidas en el Patch Tuesday, 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
- CVE-2020-17087 Detail
- CVE-2020-15999 Detail


## 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?