# Actualización de Seguridad de Microsoft - Marzo 2021

BCSC-ACTUALIZACION-MICROSOFT-2021-MARZO

TLP:WHITE

www.basquecybersecurity.eus

Marzo 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:

# 1. RESUMEN EJECUTIVO

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

En esta nueva publicación, que es acumulativa ya que incluye las graves vulnerabilidades en Exchange reportadas hace tan sólo unos días, se han corregido 89 vulnerabilidades que afectan a productos tales como los navegadores Explorer y Edge, Azure, la suite de Microsoft Office (Excel, Sharepoint, Visio,…), Windows Installer, Windows Update Stack,…

Se trata de 14 vulnerabilidades críticas y 75 clasificadas como importantes. Entre todas ellas se han reportado dos vulnerabilidades Zero-day divulgadas públicamente. Al menos una de ellas habría sido activamente explotada y utilizada en ataques.

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

## 2. RECURSOS AFECTADOS

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

- Application Virtualization
- Azure
- Azure Sphere
- Internet Explorer
- Microsoft ActiveX
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office PowerPoint
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft Windows Codecs Library
- Power BI
- Role: DNS Server
- Role: Hyper-V
- Visual Studio
- Visual Studio Code
- Windows Admin Center
- Windows Container Execution Agent
- Windows DirectX
- Windows Error Reporting
- Windows Event Tracing
- Windows Extensible Firmware Interface
- Windows Folder Redirection
- Windows Installer
- Windows Media
- Windows Overlay Filter
- Windows Print Spooler Components

- Windows Projected File System Filter Driver
- Windows Registry
- Windows Remote Access API
- Windows Storage Spaces Controller
- Windows Update Assistant
- Windows Update Stack
- Windows UPnP Device Host
- Windows User Profile Service
- Windows WalletService
- Windows Win32K

## 3. ANÁLISIS TÉCNICO

Entre las vulnerabilidades reportadas por Microsoft en este Patch Tuesday de marzo de 2021 se han publicado dos nuevos Zero Day, uno de los cuáles habría sido explotado en ataques

Descubierta en febrero por la firma de Ciberseguridad surcoreana "Enki", la vulnerabilidad de corrupción de memoria en Internet Explorer **CVE-2021-26411** habría sido utilizada por atacantes para instalar backdoors personalizados.

Por otro lado, en enero fue hecha pública por parte de la Iniciativa Zero Day de Trend Micro la vulnerabilidad de elevación de privilegios en Windoes Win32k **CVE-2021-27077**. No se tiene constancia de explotación activa de este fallo, que se ha solucionado ahora tras indicar inicialmente Microsoft que no habría solución para el mismo.

Ambos Zero Day quedan solucionados tras la actualización de seguridad publicada en este Patch Tuesday de marzo de 2021.

Además, esta actualización es acumulativa ya que incluye las correcciones ya publicadas hace unos días por Microsoft para el conjunto de vulnerabilidades conocido como **ProxyLogon** (CVE-2021-26855, 2021-26857, CVE-2021-26858 y CVE-2021-27065) que habría permitido a atacantes entrar en los servidores Microsoft Exchange de los entornos objetivo para, posteriormente, permitir la instalación de puertas traseras no autorizadas basadas en la web para facilitar el acceso a largo plazo. Según las informaciones publicadas, numerosas organizaciones se habrían visto afectadas por este fallo de seguridad hasta el momento.

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

**Vulnerabilidades Críticas**

- CVE-2021-27074 Vulnerabilidad de ejecución de código sin firma en Azure Sphere
- CVE-2021-27080 Vulnerabilidad de ejecución de código sin firma en Azure Sphere
- CVE-2021-26411 Vulnerabilidad de corrupción de memoria en Internet Explorer
- CVE-2021-26412 Vulnerabilidad de ejecución de código remoto en Microsoft Exchange Server
- CVE-2021-27065 Vulnerabilidad de ejecución de código remoto en Microsoft Exchange Server
- CVE-2021-26857 Vulnerabilidad de ejecución de código remoto en Microsoft Exchange Server

- CVE-2021-26855 Vulnerabilidad de ejecución de código remoto en Microsoft Exchange Server
- CVE-2021-26876 Vulnerabilidad de ejecución de código remoto en OpenType Font Parsing
- CVE-2021-24089 Vulnerabilidad de ejecución de código remoto en HEVC Video Extensions
- CVE-2021-27061 Vulnerabilidad de ejecución de código remoto en HEVC Video Extensions
- CVE-2021-26902 Vulnerabilidad de ejecución de código remoto en HEVC Video Extensions
- CVE-2021-26897 Vulnerabilidad de ejecución de código remoto en Windows DNS Server
- CVE-2021-26867 Vulnerabilidad de ejecución de código remoto en Windows Hyper-V
- CVE-2021-21300 Vulnerabilidad de ejecución de código remoto en Git for Visual Studio

**Vulnerabilidades Importantes:**

- CVE-2021-26890 Vulnerabilidad de ejecución de código remoto en Application Virtualization
- CVE-2021-27075 Vulnerabilidad de exposición de información en Azure Virtual Machine
- CVE-2021-27085 Vulnerabilidad de ejecución de código remoto en Internet Explorer
- CVE-2021-26869 Vulnerabilidad de exposición de información en Windows ActiveX Installer Service
- CVE-2021-27078 Vulnerabilidad de ejecución de código remoto en Microsoft Exchange Server
- CVE-2021-26854 Vulnerabilidad de ejecución de código remoto en Microsoft Exchange Server
- CVE-2021-26858 Vulnerabilidad de ejecución de código remoto en Microsoft Exchange Server
- CVE-2021-26863 Vulnerabilidad de elevación de privilegios en Windows Win32k
- CVE-2021-27077 Vulnerabilidad de elevación de privilegios en Windows Win32k
- CVE-2021-26861 Vulnerabilidad de ejecución de código remoto en Windows Graphics Component

- CVE-2021-26875 Vulnerabilidad de elevación de privilegios en Windows Win32k
- CVE-2021-26868 Vulnerabilidad de elevación de privilegios en Windows Win32k
- CVE-2021-24108 Vulnerabilidad de ejecución de código remoto en Microsoft Office
- CVE-2021-27058 Vulnerabilidad de ejecución de código remoto en Microsoft Office ClickToRun
- CVE-2021-27059 Vulnerabilidad de ejecución de código remoto en Microsoft Office
- CVE-2021-27053 Vulnerabilidad de ejecución de código remoto en Microsoft Excel
- CVE-2021-27054 Vulnerabilidad de ejecución de código remoto en Microsoft Excel
- CVE-2021-27057 Vulnerabilidad de ejecución de código remoto en Microsoft Office
- CVE-2021-27056 Vulnerabilidad de ejecución de código remoto en Microsoft PowerPoint
- CVE-2021-27052 Vulnerabilidad de exposición de información en Microsoft SharePoint Server
- CVE-2021-24104 Vulnerabilidad de spoofing en Microsoft SharePoint
- CVE-2021-27076 Vulnerabilidad de ejecución de código remoto en Microsoft PowerPoint Server
- CVE-2021-27055 Vulnerabilidad de bypass en los sistemas de seguridad de Microsoft Visio
- CVE-2021-27050 Vulnerabilidad de ejecución de código remoto en HEVC Video Extensions
- CVE-2021-27049 Vulnerabilidad de ejecución de código remoto en HEVC Video Extensions
- CVE-2021-26884 Vulnerabilidad de exposición de información en Windows Media Photo Codec
- CVE-2021-27051 Vulnerabilidad de ejecución de código remoto en HEVC Video Extensions
- CVE-2021-27062 Vulnerabilidad de ejecución de código remoto en HEVC Video Extensions
- CVE-2021-24110 Vulnerabilidad de ejecución de código remoto en HEVC Video Extensions

- CVE-2021-27048 Vulnerabilidad de ejecución de código remoto en HEVC Video Extensions
- CVE-2021-27047 Vulnerabilidad de ejecución de código remoto en HEVC Video Extensions
- CVE-2021-26859 Vulnerabilidad de exposición de información en Microsoft Power BI
- CVE-2021-27063 Vulnerabilidad de denegación de servicio en Windows DNS Server
- CVE-2021-26893 Vulnerabilidad de ejecución de código remoto en Windows DNS Server
- CVE-2021-26894 Vulnerabilidad de ejecución de código remoto en Windows DNS Server
- CVE-2021-26895 Vulnerabilidad de ejecución de código remoto en Windows DNS Server
- CVE-2021-26896 Vulnerabilidad de denegación de servicio en Windows DNS Server
- CVE-2021-26877 Vulnerabilidad de ejecución de código remoto en Windows DNS Server
- CVE-2021-26879 Vulnerabilidad de denegación de servicio en Windows NAT
- CVE-2021-27084 Vulnerabilidad de ejecución de código remoto en Visual Studio Code Java Extension Pack
- CVE-2021-27060 Vulnerabilidad de ejecución de código remoto en Visual Studio Code
- CVE-2021-27081 Vulnerabilidad de ejecución de código remoto en Visual Studio Code ESLint Extension
- CVE-2021-27083 Vulnerabilidad de ejecución de código remoto en Remote Development Extension for Visual Studio
- CVE-2021-27082 Vulnerabilidad de ejecución de código remoto en Quantum Development Kit for Visual Studio Code
- CVE-2021-27066 Vulnerabilidad de bypass en los sistemas de seguridad de Windows Admin Center
- CVE-2021-26891 Vulnerabilidad de elevación de privilegios en Windows Container Execution Agent
- CVE-2021-26865 Vulnerabilidad de elevación de privilegios en Windows Container Execution Agent
- CVE-2021-24095 Vulnerabilidad de elevación de privilegios en DirectX

- CVE-2021-24090 Vulnerabilidad de elevación de privilegios en Windows Error Reporting
- CVE-2021-24107 Vulnerabilidad de exposición de información en Windows Event Tracing
- CVE-2021-26872 Vulnerabilidad de elevación de privilegios en Windows Event Tracing
- CVE-2021-26901 Vulnerabilidad de elevación de privilegios en Windows Event Tracing
- CVE-2021-26898 Vulnerabilidad de elevación de privilegios en Windows Event Tracing
- CVE-2021-26892 Vulnerabilidad de bypass en los sistemas de seguridad de Windows Extensible Firmware Interface
- CVE-2021-26887 Vulnerabilidad de elevación de privilegios en Microsoft Windows Folder Redirection
- CVE-2021-26862 Vulnerabilidad de elevación de privilegios en Windows Installer
- CVE-2021-26881 Vulnerabilidad de ejecución de código remoto en Microsoft Windows Media Foundation
- CVE-2021-26874 Vulnerabilidad de elevación de privilegios en Windows Overlay Filter
- CVE-2021-26860 Vulnerabilidad de elevación de privilegios en Windows App-V Overlay Filter
- CVE-2021-1640 Vulnerabilidad de elevación de privilegios en Windows Print Spooler
- CVE-2021-26878 Vulnerabilidad de elevación de privilegios en Windows Print Spooler
- CVE-2021-26870 Vulnerabilidad de elevación de privilegios en Windows Projected File System
- CVE-2021-26864 Vulnerabilidad de elevación de privilegios en Windows Virtual Registry Provider
- CVE-2021-26882 Vulnerabilidad de elevación de privilegios en Remote Access API
- CVE-2021-26880 Vulnerabilidad de elevación de privilegios en Storage Spaces Controller
- CVE-2021-27070 Vulnerabilidad de elevación de privilegios en Windows 10 Update Assistant
- CVE-2021-1729 Vulnerabilidad de elevación de privilegios en Windows Update Stack Setup

- CVE-2021-26889 Vulnerabilidad de elevación de privilegios en Windows Update Stack
- CVE-2021-26866 Vulnerabilidad de elevación de privilegios en Windows Update Service
- CVE-2021-26899 Vulnerabilidad de elevación de privilegios en Windows UPnP Device Host
- CVE-2021-26873 Vulnerabilidad de elevación de privilegios en Windows User Profile Service
- CVE-2021-26886 Vulnerabilidad de denegación de servicio en User Profile Service Denia
- CVE-2021-26871 Vulnerabilidad de elevación de privilegios en Windows WalletService
- CVE-2021-26885 Vulnerabilidad de elevación de privilegios en Windows WalletService
- CVE-2021-26900 Vulnerabilidad de elevación de privilegios en Windows Win32k

# 4. MITIGACIÓN / SOLUCIÓN

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

# 5. REFERENCIAS ADICIONALES

- March 2021 Security Updates
- Security update deployment information: March 10, 2020 (microsoft.com)
- Security Update Guide - Microsoft
- BCSC – Actualización Seguridad Servidores Exchange


## 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?