BOLETÍN DE ALERTA

Boletín Nro.: 2020-27

Fecha de publicación: 11/09/2020

Tema: Microsoft aborda vulnerabilidades de riesgo crítico, alto y medio en actualizaciones de seguridad para varios de sus productos

Los identificadores son los siguientes:

Vulnerabilidades catalogadas de riesgo **crítico** son: CVE-2020-0878, CVE-2020-16857, CVE-2020-16862, CVE-2020-16875, CVE-2020-1285, CVE-2020-1210, CVE-2020-1595, CVE-2020-1200, CVE-2020-1576, CVE-2020-1452, CVE-2020-1453, CVE-2020-1460, CVE-2020-1057, CVE-2020-1172, CVE-2020-1593, CVE-2020-0922, CVE-2020-1252, CVE-2020-1508, CVE-2020-0908, CVE-2020-1319, CVE-2020-0997, CVE-2020-1129, CVE-2020-16874 .

Vulnerabilidades catalogadas como de **riesgo alto más resaltantes** son: CVE-2020-0761, CVE-2020-0718, CVE-2020-16860, CVE-2020-1039, CVE-2020-1074, CVE-2020-1338, CVE-2020-1332, CVE-2020-1218, CVE-2020-1193, CVE-2020-1012, CVE-2020-1506, CVE-2020-0921, CVE-2020-0998, CVE-2020-1152, CVE-2020-1245, CVE-2020-0838, CVE-2020-16853, CVE-2020-16851, CVE-2020-16852, CVE-2020-1034.

Vulnerabilidad catalogada como de **riesgo medio** es: CVE-2020-1044

Sistemas afectados:

- Microsoft Windows 10, Windows 8.1, Windows 7, Windows Server 2008, Windows Server 2012, Windows Server 2016 y Windows Server 2019
- Microsoft Edge (EdgeHTML-based)
- Microsoft ChakraCore
- Internet Explorer
- Microsoft Dynamics
- Visual Studio
- Microsoft Exchange Server
- Microsoft Windows Codecs Library
- Microsoft Windows

- Microsoft Jet Database Engine
- SQL Server
- ASP.NET Core
- Microsoft Office, Microsoft Office Services y Microsoft Web Apps
- Microsoft Sharepoint
- Microsoft NTFS
- Microsoft OneDrive
- Windows Hyper-V
- Windows Kernel
- Active Directory
- Microsoft Graphics

Puede verse una descripción completa de los productos y servicios afectados en el siguiente enlace: https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Sep

Descripción:

Microsoft ha lanzado actualizaciones de seguridad, correspondientes al **Patch Tuesday** de Setiembre, en donde abordan **129 vulnerabilidades**, de las cuales **23** han sido catalogadas como **críticas**, **105** de **riesgo alto** y **1** de **riesgo medio**.

A continuación se detallan brevemente las 23 vulnerabilidades de riesgo crítico abordadas:

Múltiples vulnerabilidades de **ejecución remota de código** que se dan debido a un **mal manejo de objetos en memoria**:

- Los CVE-2020-1057 y CVE-2020-1172, afectan al **motor de script ChakraCore** del navegador **Microsoft Edge (EdgeHTML-based)** para los sistemas **Windows (ver versiones específicas afectadas)**
- Por otro lado, el CVE-2020-0922 afecta a **Microsoft COM** para los sistemas **Windows 10, Windows 8, Windows 7, Windows Server 2008, 2012, 2016 y 2019 (ver versiones específicas afectadas)**

- El CVE-2020-1252, afecta a **Microsoft Windows 10, Windows 8, Windows 7, Windows Server 2008, 2012, 2016 y 2019 (ver versiones específicas afectadas)**.
- El CVE-2020-0908, afecta al módulo **Windows Text Service** para los sistemas **Windows 10, Windows Server 2016 y 2019 (ver versiones específicas afectadas)**.
- El CVE-2020-0997, afecta al códec de la **Windows Camera** de los sistemas **Windows 10, Windows Server 2016 y 2019 (ver versiones específicas afectadas)**.
- El CVE-2020-1129, afecta a la librería **Microsoft Windows Codecs** para los sistemas **Windows 10, Windows Server 2016 y 2019 (ver versiones específicas afectadas)**.
- El CVE-2020-0878, afecta a los navegadores web **Internet Explorer 11** y **Microsoft Edge (EdgeHTML-based)** para los sistemas **Windows (ver versiones específicas afectadas)**.

- Por otro lado, el CVE-2020-1285 afecta al componente **Windows Graphics Device Interface (GDI)** de los sistemas **Windows 10, Windows 8, Windows 7, Windows Server 2008, 2012, 2016 y 2019 (ver versiones específicas afectadas)**;
- Y finalmente el CVE-2020-16874, afecta a **Microsoft Visual Studio (ver versiones específicas afectadas)**.

Por otro lado el CVE-2020-16857, afecta a **Microsoft Dynamics 365 for Finance and Operations** en su **versión 10.0.11** y se da debido a un mal manejo de la entrada de datos proporcionada por el usuario. Un atacante remoto con privilegios para importar y exportar datos podría explotar exitosamente este fallo enviando un archivo especialmente diseñado al **servidor Dynamics** vulnerable.

Mientras que el CVE-2020-16862, afecta a **Microsoft Dynamics 365** en su **versión 9.0**, y es debido a que el servidor no sanitiza correctamente las solicitudes web recibidas. La explotación exitosa de este fallo permitiría a un atacante remoto ejecutar código en el contexto de la cuenta de servicio SQL.

El CVE-2020-16875, afecta a **Microsoft Exchange Server 2016 (ver versiones específicas afectadas)** y se da debido a una validación inapropiada de los **argumentos cmdlet.** La explotación exitosa permitiría a un atacante autenticado con un rol de Exchange, ejecutar

código en el contexto del usuario System.

Los CVE-2020-1210, CVE-2020-1200, CVE-2020-1576, CVE-2020-1452, CVE-2020-1453 afectan a **Microsoft Sharepoint** y se dan debido a que el software no verifica el código fuente de un paquete de aplicación. Un atacante remoto podría explotar exitosamente este fallo cargando un **paquete de aplicación Sharepoint** especialmente diseñado a una versión afectada. Los **productos afectados** son:

- Microsoft SharePoint Enterprise Server 2013, 2016
- Microsoft SharePoint Foundation 2010, 2013
- Microsoft SharePoint Server 2010, 2019
- Microsoft SharePoint Enterprise Server 2013, 2016
- Microsoft Business Productivity Servers 2010

Mientras que CVE-2020-1595, afecta a **Microsoft Sharepoint Enterprise Server 2013 y 2016; Sharepoint Foundation 2013 y Sharepoint Server 2019.** Este fallo se da debido a que las APIs no protegen correctamente de datos inseguros proveídos por el usuario. La explotación exitosa permitiría a un atacante ejecutar código en el contexto del grupo de aplicaciones Sharepoint y la cuenta de los servidores de Sharepoint.

El CVE-2020-1460, afecta a **Microsoft Sharepoint Server (ver versiones específicas afectadas)** y se da debido a que el servidor no identifica y filtra correctamente **controles web ASP.Net inseguros**. La explotación exitosa de este fallo permitiría a un atacante utilizar una página especialmente diseñada para realizar acciones arbitrarias en el contexto del grupo de aplicaciones Sharepoint.

Finalmente los CVE-2020-1593 y CVE-2020-1508, afectan al **códec de audio** de **Windows Media** para los sistemas **Windows 10, Windows 8, Windows 7, Windows Server 2008, 2012, 2016 y 2019 (ver versiones específicas afectadas)** y se dan debido a un manejo inapropiado de objetos. Un atacante podría explotar exitosamente este fallo convenciendo a la víctima para que abra un documento especialmente diseñado, o que visite una página maliciosa.

Así también se describen a continuación las vulnerabilidades más resaltantes de riesgo alto y medio:

Múltiples vulnerabilidades de **ejecución remota de código** en **Active Directory** (CVE-2020-0761, CVE-2020-0718), **Microsoft Dynamics** (CVE-2020-16860), **Microsoft Jet Database Engine** (CVE-2020-1039, CVE-2020-1074) y **Microsoft Office para Windows** (CVE-2020-1338, CVE-2020-1332, CVE-2020-1218, CVE-2020-1193). Fallos que permitirían a un atacante **escalar privilegios** en **Internet Explorer** (CVE-2020-1012, CVE-2020-1506), **Microsoft Graphics** (CVE-2020-0921, CVE-2020-0998, CVE-2020-1152, CVE-2020-1245) , **Microsoft NTFS** (CVE-2020-0838), **Microsoft OneDrive para Windows** (CVE-2020-16853, CVE-2020-16851, CVE-2020-16852), **Kernel de Windows** (CVE-2020-1034) y un fallo de riesgo medio en **SQL Server** (CVE-2020-1044) que permitiría a un atacante autenticado **cargar tipos de archivos no permitidos** por el administrador.

Impacto:

La explotación exitosa de estas vulnerabilidades, permitiría a un atacante:

- Instalar programas maliciosos, ver, cambiar o eliminar datos, crear cuentas de usuarios obtener información y tomar el control total del recurso afectado;
- Ejecutar código remoto en el sistema afectado;
- Escalar privilegios;
- Realizar ataques de denegación de servicios (DoS).

Solución y prevención:

- Aplicar la actualización de seguridad, desde el apartado "**Security Updates**" de la página oficial de Microsoft, para los siguientes productos afectados:
    - **Internet Explorer 11**, desde el siguiente enlace;
    - **Microsoft ChakraCore**, desde el siguiente enlace;
    - **Visual Studio**, desde el siguiente enlace;
    - **Microsoft Exchange Server**, desde el siguiente enlace;
    - **Microsoft Sharepoint**, desde el siguiente enlace;
    - **SQL Server**, desde el siguiente enlace;

- **Microsoft OneDrive**, desde el siguiente enlace;
- **Microsoft Dynamics**, desde el siguiente enlace;
- **Microsoft Office**, desde el siguiente enlace.

- Aplicar los **parches de seguridad** correspondientes a cada sistema operativo, para ello dirigirse al menú de **Ajustes (Settings) > Actualización y seguridad (Update & Security) > Actualización de Windows (Windows Update) > Revisar actualizaciones (Check for updates)** y la actualización se descargara e instalara automáticamente.

Más detalles y recomendaciones pueden ser visualizados en el aviso de seguridad oficial de Microsoft.

Información adicional:

- https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Sep
- https://www.bleepingcomputer.com/news/microsoft/microsoft-september-2020-patch-tuesday-fixes-129-vulnerabilities/
- https://thehackernews.com/2020/09/patch-tuesday-september.html
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/boletin-seguridad-microsoft-septiembre-2020