BOLETÍN DE ALERTA

Boletín Nro.: 2020-14
Fecha de publicación: 19/05/2020
Tema: Actualizaciones de seguridad de Microsoft abordan 111 vulnerabilidades catalogadas como críticas, altas y de riesgo medio.

Las vulnerabilidades catalogadas como **críticas** son: CVE-2020-1056, CVE-2020-1153, CVE-2020-1117, CVE-2020-1069, CVE-2020-1102, CVE-2020-1024, CVE-2020-1023, CVE-2020-1065, CVE-2020-1037, CVE-2020-1028,CVE-2020-1136, CVE-2020-1126, CVE-2020-1192.

Productos afectados:

- Microsoft Windows;
- Microsoft Edge (EdgeHTML-based);
- Microsoft Edge (Chromium-based);
- ChakraCore;
- Internet Explorer;
- Microsoft Office and Microsoft Office Services and Web Apps;
- Windows Defender;
- Visual Studio;
- Microsoft Dynamics;
- .NET Framework;
- .NET Core;
- Power BI

Descripción:

Recientemente Microsoft ha lanzado actualizaciones de seguridad, las mismas abordan un total de **111 vulnerabilidades**, siendo **13** de estas de riesgo **crítico**, **91** de **alto** riesgo, **3** de **medio** riesgo y **4** de **bajo** riesgo.

A continuación se detallan las **13 vulnerabilidades** catalogadas como **críticas**:

El CVE-2020-1056, se trata de un fallo en **Microsoft Edge**, y es debido a una aplicación indebida de las políticas entre dominios, sabiendo esto un atacante podría diseñar especialmente un sitio web y engañar a la víctima con el fin de que esta ingrese al enlace malicioso, provocando una **escalada de privilegios**. Afecta a: Windows 10 (Se puede ver la versión específica Aquí), Windows Server 2016 y Windows Server 2019.

El CVE-2020-1153, se da en **Microsoft Graphic Components**, y es debido a un mal manejo de los objetos en memoria. Sabiendo esto, un atacante podría engañar a la víctima con el fin de que este abra un archivo malicioso especialmente diseñado, lo que resultaría en una **ejecución remota de código**. Afecta a:

- Windows 10,
- Windows 8,
- Windows 7,
- Windows Server 2019,
- Windows Server 2016,
- Windows Server 2012,
- Windows Server 2008,
- Se puede visualizar las versiones específicas afectadas en el siguiente enlace.

El CVE-2020-1117, se trata de un fallo en **Microsoft Color Management**, y es debido a un manejo indebido de los objetos en memoria por parte del módulo **Color Management** (**ICM32.dll**). Con esto, un atacante podría engañar a la víctima con el fin de que ingrese a un sitio web especialmente diseñado (enlaces adjuntos a un correo electrónico o mensaje), resultando en una **ejecución remota de código** en el sistema. Este fallo afecta a **Windows 10**, **Windows Server 2019**, **Windows Server 2016**, se puede visualizar las versiones específicas afectadas Ver**.**

Por otro lado, 4 vulnerabilidades **críticas** en **Microsoft Sharepoint.** La **primera** (CVE-2020-1069) se trata de un fallo en la identificación y filtrado de "**ASP.net web controls**". Mientras que, la **segunda** (CVE-2020-1102), la **tercera** (CVE-2020-1024) y la **cuarta** (CVE-2020-1023) se deben a un fallo en la verificación de la fuente "**markup**" de un paquete de aplicación. La explotación exitosa de estas vulnerabilidades permitiría a un atacante la **ejecución remota de código**. Afecta a:

- Microsoft SharePoint Enterprise Server 2019,
- Microsoft Sharepoint Server 2019,

- Microsoft SharePoint Enterprise Server 2016 y
- Microsoft SharePoint Foundation 2013 Service Pack 1.

Mientras que el CVE-2020-1065, se debe a un manejo indebido de los objetos en memoria por parte de **ChakraCore Scripting Engine**, provocando una corrupción de la memoria que podría llevar a una **ejecución remota de código**. Afecta a: **Windows 10** (Se puede ver la versión específica Aquí) y **Windows Server 2019**.

El CVE-2020-1037, se debe a un fallo en **Microsoft Edge** (**HTML-based**), específicamente un manejo indebido de objetos en la memoria, provocando una corrupción de la memoria que podría llevar a una **ejecución remota de código**. Afecta a:

- Windows 10 (Se puede ver la versión específica en: Ver),
- Windows Server 2019 y
- Windows Server 2016.

Los CVE-2020-1028, CVE-2020-1136 y CVE-2020-1126, se deben un manejo indebido de objetos en memoria por parte de **Windows Media Foundation** y de ser explotadas exitosamente permitirían a un atacante instalar programas, cambiar o eliminar datos e inclusive crear cuentas con **permisos de administrador**. Afecta a:

- Windows 10 (se puede ver la versión específica en: Ver),
- Windows 8 (se puede ver la versión específica en: Ver),
- Windows Server 2019 (se puede ver la versión específica en: Ver),
- Windows Server 2016 (se puede ver la versión específica en: Ver) y
- Windows Server 2012 (se puede ver la versión específica en: Ver).

El CVE-2020-1192, se trata de un fallo en **Visual Studio Code**, específicamente cuando la **extensión de Python** carga las configuraciones del espacio de trabajo a través de un **archivo notebook**. La explotación exitosa de este fallo permitiría a un atacante la **ejecución remota de código**.

Por otro lado, las vulnerabilidades de **riesgo alto** afectan a los siguientes productos:

- .NET Core,
- .NET Framework,
- Microsoft Dynamics,
- Microsoft Edge,
- Microsoft Graphics Component,

- Microsoft Jet Database Engine,
- Microsoft Office,
- Microsoft Office SharePoint,
- Microsoft Windows,
- Power BI y
- Visual Studio.

El CVE-2020-1067 afecta a Microsoft **Windows**, el CVE-2020-1096 afecta a **Microsoft Edge** PDF. Los CVE-2020-1051, CVE-2020-1174, CVE-2020-1175 y CVE-2020-1176 afectan a **Jet Database Engine** y el CVE-2020-0901 afecta a **Microsoft Excel**. Son algunas de las vulnerabilidades de **alto riesgo** abordadas y que en caso de ser explotadas exitosamente permitirían a un atacante la **ejecución de código remoto**.
Otras vulnerabilidades también catalogadas como **altas**, que afectan a **.NET Core** y **.NET Framework** son los CVE-2020-1108, CVE-2020-1161 y CVE-2020-1066. En caso de ser explotadas exitosamente permitirían a un atacante **escalar privilegios** y realizar ataques de **denegación de servicios (DoS).**

Además, Microsoft ha lanzado otra actualización de seguridad el cual aborda una vulnerabilidad de riesgo **alto**, la misma ha sido identificada con el CVE-2020-0655, y afecta a los **servicios de escritorio remoto** de sus sistemas **Windows.** Este fallo se da cuando un atacante autenticado abusa de la redirección del portapapeles, resultando en un **ejecución remota de código**. Afecta a:

- Windows 10,
- Windows 8,
- Windows 7,
- Windows Server 2019,
- Windows Server 2016,
- Windows Server 2012 y
- Windows Server 2008.

Obs: las **versiones específicas** de los sistemas afectados pueden ser visualizadas aquí**.**

Impacto:

La explotación exitosa de estos fallos, permitirían a un atacante:

- Instalar programas maliciosos, ver, cambiar o eliminar datos, crear cuentas de usuarios y tomar el control total del recurso afectado,
- Escalar privilegios y
- Ejecutar código remoto en el sistema afectado.

Solución y prevención:

- Aplicar la **actualización de seguridad** para **Microsoft Edge** desde el apartado "**Security Updates"** de la página oficial de Microsoft.
- Actualizar **ChakraCore** a la **versión** 1.11.19.
- Para el caso **Microsoft Sharepoint**, aplicar los parches dependiendo del sistema afectado:
    - Actualizar **Microsoft Sharepoint Server 2016** a la última versión disponible.
    - Actualizar **Microsoft Sharepoint Foundation 2013** a la última versión disponible.
    - Actualizar **Microsoft SharePoint Server 2019** a la última versión disponible.
- Aplicar la **actualización de seguridad** para **Microsoft Windows** desde el apartado "**Security Updates"** de la página oficial de Microsoft.
- Aplicar los parches de seguridad correspondientes a cada sistema operativo, 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-May
- https://www.zdnet.com/article/microsoft-may-2020-patch-tuesday-fixes-111-vulnerabilities/
- https://www.bleepingcomputer.com/news/microsoft/may-2020-patch-tuesday-microsoft-fixes-111-vulnerabilities-13-critical/