BOLETÍN DE ALERTA

Boletín Nro.: 2020-17
Fecha de publicación: 10/06/2020
Tema: Microsoft aborda actualizaciones de seguridad 129 vulnerabilidades 11 de ellas consideradas como críticas y 118 de alto riesgo

La vulnerabilidades catalogadas como **críticas** son: CVE-2020-9633, CVE-2020-1219, CVE-2020-1181, CVE-2020-1073, CVE-2020-1216, CVE-2020-1213, CVE-2020-1248, CVE-2020-1281, CVE-2020-1300, CVE-2020-1299 y CVE-2020-1286.

Productos afectados:

- Microsoft Windows;
- Microsoft Edge (EdgeHTML-based);
- Microsoft Edge (Chromium-based) in IE Mode;
- Microsoft ChakraCore;
- Internet Explorer;
- Microsoft Office and Microsoft Office Services and Web Apps;
- Windows Defender;
- Microsoft Dynamics;
- Azure DevOps;
- HoloLens;
- Adobe Flash Player;
- Windows App Store;
- System Center;

Descripción:

Recientemente Microsoft ha lanzado actualizaciones de seguridad correspondientes al **Patch Tuesday** de Junio, las mismas abordan un total de **129 vulnerabilidades**, siendo **11** de estas de riesgo **crítico**, **118** de riesgo **alto**.

A continuación se detallan las **11 vulnerabilidades** catalogadas como **críticas**:

Los CVE-2020-1219 y CVE-2020-1073, se dan en los navegadores de Microsoft (**Internet Explorer, Microsoft Edge**) y en el intérprete de javascript **ChakraCore**, debido a que estos

manejan inadecuadamente los objetos en memoria. La explotación exitosa de esta vulnerabilidad permitiría a un atacante la **ejecución remota de código** en el contexto del usuario actual. Afecta a:

- Windows 10,
- Windows 8,
- Windows 7,
- Windows Server 2019,
- Windows Server 2016,
- Se pueden visualizar las versiones específicas afectadas en el apartado **Security Updates** del siguiente **enlace**.

El **CVE-2020-1181**, se da en **Microsoft Sharepoint Server**, debido a un fallo de identificaicon y filtracion de controles **ASP.Net** inseguros. La explotación exitosa de esta vulnerabilidad permitiría a un atacante autenticado utilizar una **página maliciosa** diseñada especialmente para realizar acciones en el contexto de seguridad del proceso de grupo de aplicaciones en SharePoint. Afecta a: Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Foundation 2010 Service Pack 2, Microsoft SharePoint Foundation 2013 Service Pack 1 y Microsoft SharePoint Server 2019.

Por otro lado, el **CVE-2020-9633** se trata de una vulnerabilidad **use-after-free** en **Adobe Flash Player** que afecta a las versiones **32.0.0.371** y **anteriores** para **Windows.** La explotación exitosa de esta vulnerabilidad permitiría a un atacante realizar un ataque de **Denegación de Servicios(DoS).** Afecta a:

- Windows 10,
- Windows 8,
- Windows Server 2019,
- Windows Server 2016,
- Windows Server 2012,
- Se pueden visualizar las versiones específicas afectadas en el apartado **Security Updates** del siguiente **enlace**.

Los CVE-2020-1216 y CVE-2020-1213, se dan en el lenguaje de script **VBScript,** debido a que maneja inadecuadamente objetos en memoria. La explotación exitosa **ejecutar código remoto** en el contexto del usuario actual. Afecta:

- Windows 10,
- Windows 8,
- Windows 7,
- Windows Server 2019,
- Windows Server 2016,
- Windows Server 2008,
- Se pueden visualizar las versiones específicas afectadas en el apartado **Security Updates** del siguiente **enlace.**

Mientras que el CVE-2020-1248, se da en **Windows Graphics Device Interface (GDI),** debido a que maneja inadecuadamente objetos en memoria. Un atacante podría utilizar un **sitio web** o **archivo** especialmente diseñado para explotar la vulnerabilidad y convencer a la víctima para que ingrese al sitio o descargue el archivo, llevando a una **ejecución remota de código** en el contexto del usuario víctima. Afecta a: Windows 10 y Windows Server, se pueden visualizar las versiones específicas en el siguiente **enlace.**

El CVE-2020-1281, se da en **Microsoft Windows OLE,** debido a una validación errónea de los datos de entrada proveídos por el usuario. Con esto, un atacante podría convencer a un usuario a abrir un **archivo malicioso** o **programa** desde una página web o enviado por un correo electrónico, la explotación exitosa permitirá 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 pueden visualizar las versiones específicas afectadas en el apartado **Security Updates** del siguiente **enlace.**

El CVE-2020-1300, se da en **Microsoft Windows**, debido a un manejo inapropiado de archivos del tipo **cabinet.** Un atacante podría explotar exitosamente esta vulnerabilidad convenciendo a un usuario que abra un archivo **cabinet** malicioso especialmente diseñado para explotar la vulnerabilidad y de tener éxito llevar a 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 pueden visualizar las versiones específicas afectadas en el apartado **Security Updates** del siguiente **enlace.**

EL CVE-2020-1299, se da en **Microsoft Windows** durante el procesamiento de un archivo del tipo **.LNK**, un atacante podría explotar esta vulnerabilidad con privilegios del usuario, engañándolo para que abra un archivo .LNK asociado con **binarios maliciosos** y una vez dicho archivo sea analizado por **Windows Explorer** o cualquier otra herramienta analizadora de archivos .LNK **ejecutar código malicioso** en el sistema. Afecta a:

- Windows 10,
- Windows 8,
- Windows 7,
- Windows Server 2019,
- Windows Server 2016,
- Windows Server 2012,
- Windows Server 2008,
- Se pueden visualizar las versiones específicas afectadas en el apartado **Security Updates** del siguiente **enlace.**

Finalmente, el CVE-2020-1286 se da en **Windows Shell** debido a una validación errónea de la **ruta de archivos**. Un atacante podría convencer a un usuario que abra un archivo malicioso

especialmente diseñado para explotar la vulnerabilidad y de tener éxito **ejecutar código remoto** en el contexto del usuario víctima. Afecta a: **Windows 10** y **Windows Server**, se pueden visualizar las versiones específicas afectadas en el siguiente **enlace**.

SMBleed

También fue abordada una vulnerabilidad de riesgo **alto** reconocida como **SMBleed** e identificada como **CVE-2020-1206**.

Este fallo afecta al protocolo **SMB (Server Message Block) versión 3.1.1** que sirve para compartir archivos y comunicarse entre nodos de una red de computadoras, específicamente en la función "**Srv2DecompressData**" debido a que maneja de forma indebida las solicitudes recibidas. Con esto un atacante podría enviar un paquete malicioso especialmente diseñado para explotar la vulnerabilidad a un servidor que esté utilizando **SMBv3**, permitiéndole leer datos no inicializados de la memoria del kernel y realizar modificaciones en la función de compresión obteniendo así información confidencial que podría servir para comprometer al sistema.

Para explotar esta vulnerabilidad en el **Cliente SMBv3**, es necesario que un atacante no autenticado realice la configuración de un **servidor SMBv3** malicioso y convenza al usuario para que se conecte al mismo.

Además, de ser combinado con la vulnerabilidad **crítica SMBGhost** (CVE-2020-0796) que fue abordada hace 3 meses por Microsoft. Podría permitir a un atacante la **ejecución de remota de código**.

Esta vulnerabilidad afecta a **Windows 10** y **Windows Server**, se pueden visualizar las versiones específicas afectadas en el siguiente **enlace**.

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

- Windows Media Player
- Windows Kernel
- Visual Studio
- Microsoft Scripting Engine

- Microsoft Office SharePoint
- Microsoft Office
- Microsoft JET Database Engine
- Microsoft Graphics Component
- Microsoft Word for Android
- Windows Defender
- Navegadores Microsoft

Se detectaron vulnerabilidades de mal manejo de archivos en **Microsoft Word** para Android (**CVE-2020-1223**), filtracion de informacion confidencial en **Internet Explorer** (**CVE-2020-1315**). Así como también, múltiples debilidades en el **Kernel de Windows** (**CVE-2020-1273**, **CVE-2020-1276**, **CVE-2020-1310**), una vulnerabilidad de omisión de seguridad en **Microsoft Outlook** (**CVE-2020-1229**), múltiples errores en el manejo de objetos en memoria en **Microsoft Office** (**CVE-2020-1225**, **CVE-2020-1226**) y una vulnerabilidad de **filtración de información** debido a la exposición de **tokens** en texto plano en **Visual Studio** (**CVE-2020-1343**), son algunas de las más resaltantes.

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,
- Ejecutar código remoto en el sistema afectado y
- Obtener información confidencial.

Solución y prevención:

- Aplicar la actualización de seguridad para **Microsoft Edge** e **Internet Explorer** desde el apartado "**Security Updates**" de la **página oficial de Microsoft**.
- Para el caso de Microsoft Sharepoint, aplicar los parches dependiendo del sistema afectado:
    - Actualizar **Microsoft SharePoint Enterprise Server 2016** a la última versión

disponible,

- Actualizar **Microsoft SharePoint Foundation 2010 Service Pack 2** a la última versión disponible,
- Actualizar **Microsoft SharePoint Foundation 2013 Service Pack 1** la última versión disponible,
- Actualizar **Microsoft SharePoint Server 2019** la última versión disponible.

- Desactivar "**Compression**" para lidiar con la vulnerabilidad **SMBleed**, bloqueando el acceso al servidor a atacantes no autenticados, con el siguiente comando **PowerShell**:

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
DisableCompression -Type DWORD -Value 1 -Force
```

- 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-Jun
- https://thehackernews.com/2020/06/windows-update-june.html
- https://thehackernews.com/2020/06/SMBleed-smb-vulnerability.html
- https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2020-patch-tuesday-largest-ever-with-129-fixes/