BOLETÍN DE ALERTA

Boletín Nro.: 2020-22

Fecha de publicación: 16/07/2020

Tema: Actualizaciones de seguridad en productos de Microsoft abordan 123 vulnerabilidades, 18 de ellas catalogadas como críticas y 105 de riesgo alto.

Las vulnerabilidades catalogadas como **críticas** son: CVE-2020-1147, CVE-2020-1436, CVE-2020-1435, CVE-2020-1409, CVE-2020-1349, CVE-2020-1439, CVE-2020-1403, CVE-2020-1410, CVE-2020-1374, CVE-2020-1421, CVE-2020-1350, CVE-2020-1025, CVE-2020-1041, CVE-2020-1040, CVE-2020-1032, CVE-2020-1036, CVE-2020-1042 y CVE-2020-1043.

Productos afectados:

- Windows DNS server, de los sistemas Windows Server 2003 a 2019.
- Microsoft Windows
- Microsoft Edge (EdgeHTML-based)
- Microsoft Edge (Chromium-based) en modo IE
- Microsoft ChakraCore
- Internet Explorer
- Microsoft Office, Microsoft Office Services y Microsoft Office Web Apps
- Windows Defender
- Skype for Business
- Visual Studio
- Microsoft OneDrive
- .NET Framework
- Azure DevOps

Descripción:

Recientemente Microsoft ha lanzado actualizaciones de seguridad correspondientes al **Patch Tuesday** de Julio, las mismas abordan un total de **123 vulnerabilidades** de las cuales **18** han

sido catalogadas como **críticas** y **105** de **alto riesgo**.

A continuación, se detallan las **18 vulnerabilidades** catalogadas como **críticas**:

SigRed

Una vulnerabilidad altamente **crítica**, reconocida como **SigRed** e identificada con el CVE-2020-1350. Este fallo afecta a **Windows DNS Server** de los sistemas **Windows Server 2003 a 2019**, y se encuentra en el módulo del servidor DNS llamado **dns.exe**, específicamente en la función **dns.exe!SigWireRead**, y se da debido a que el servidor DNS no maneja correctamente las peticiones.

Además, esta vulnerabilidad puede ser explotada remotamente por un atacante a través de un navegador como **Internet Explorer** y **Microsoft Edge**, haciendo provecho de las características de **reutilización de conexión** y **query pipelining** para enviar una consulta DNS maliciosa dentro de una solicitud HTTP al servidor DNS destino cuando la víctima visita un sitio web bajo el control del atacante.

La explotación exitosa de este fallo permitiría a los atacantes obtener privilegios de administrador dentro de los servidores afectados y tomar control de la infraestructura de la organización. Además podría ocasionar una reacción en cadena permitiendo ampliar el ataque a todas las máquinas vulnerables de la red sin necesidad de interacción humana.

Una **prueba de concepto (PoC)** de la explotación de esta vulnerabilidad, lo puede visualizar en el siguiente **enlace**.

Además han sido identificadas vulnerabilidades de **ejecución remota de código**:

Los CVE-2020-1147 y CVE-2020-1439, afectan a **.NET framework**, **Microsoft Sharepoint** y **Visual Studio** (las versiones específicas afectadas pueden ser visualizadas en el apartado **"Security Updates"** del siguiente **enlace**); y se dan debido a que no se verifican correctamente el **markup** de origen de los archivos **XML**.

Mientras que los CVE-2020-1041, CVE-2020-1040, CVE-2020-1032, CVE-2020-1036, CVE-2020-1042 y CVE-2020-1043 afectan al componente **Hyper-V RemoteFX vGPU** de los sistemas **Windows Server 2008**, **Windows Server 2012** y **Windows Server 2016;** y se dan

debido a que el servidor **host** no valida correctamente las entradas proporcionadas por un usuario autenticado en el sistema operativo invitado.

Por otro lado, el **CVE-2020-1436** afecta a la librería **Windows Font** de los sistemas **Windows 10**, **Windows 7**, **Windows 8.1**, **Windows Server 2008**, **Windows Server 2012**, **Windows Server 2016** y **Windows Server 2019** (las versiones específicas afectadas pueden ser visualizadas en el apartado **"Security Updates"** del siguiente enlace); y se da debido a que dicha librería no maneja correctamente las fuentes especialmente diseñadas.

El **CVE-2020-1435**, afecta a la interfaz **Windows Graphics Device Interface (GDI)** de los sistemas **Windows 10**, **Windows 7**, **Windows 8.1**, **Windows RT**, **Windows Server 2008**, **Windows Server 2012**, **Windows Server 2016** y **Windows Server 2019** (las versiones específicas afectadas pueden ser visualizadas en el apartado **"Security Updates"** del siguiente enlace); y se da debido a un mal manejo de los objetos en memoria.

Los **CVE-2020-1403** y **CVE-2020-1349**, afectan al lenguaje de script **VBScript** de **Internet Explorer 9 y 11;** y **Microsoft Outlook** (las versiones específicas afectadas pueden ser visualizadas en el apartado **"Security Updates"** del siguiente enlace), debido a un mal manejo de los objetos en memoria.

El **CVE-2020-1410**, afecta al componente **Windows Address Book** de los sistemas **Windows 10**, **Windows 7**, **Windows 8.1**, **Windows RT 8.1**, **Windows Server 2008**, **Windows Server 2012**, **Windows Server 2016** y **Windows Server 2019** (las versiones específicas afectadas pueden ser visualizadas en el apartado "**Security Updates**" del siguiente enlace); y se da debido a un procesamiento erróneo de los **archivos vcard.**

El **CVE-2020-1409** afecta a la API **DirectWrite** de los sistemas **Windows 10**, **Windows 7**, **Windows 8.1**, **Windows RT 8.1**, **Windows Server 2008**, **Windows Server 2012**, **Windows Server 2016** y **Windows Server 2019** (las versiones específicas afectadas pueden ser visualizadas en el apartado "**Security Updates**" del siguiente enlace); y se da debido a un mal manejo de los objetos en memoria.

El **CVE-2020-1421**, se da durante el procesamiento de **archivos .LNK** específicos y afecta a los sistemas **Windows 10**, **Windows 7**, **Windows 8.1**, **Windows RT 8.1**, **Windows Server**

2008, **Windows Server 2012**, **Windows Server 2016** y **Windows Server 2019** (las versiones específicas afectadas pueden ser visualizadas en el apartado "**Security Updates**" del siguiente enlace).

El **CVE-2020-1374** afecta al cliente **Windows Remote Desktop** de los sistemas **Windows 10**, **Windows 7**, **Windows 8.1**, **Windows RT 8.1**, **Windows Server 2008**, **Windows Server 2012**, **Windows Server 2016** y **Windows Server 2019** (las versiones específicas afectadas pueden ser visualizadas en el apartado "**Security Updates**" del siguiente enlace); y se da cuando un usuario se conecta a un **servidor malicioso**.

Además, fue abordada una vulnerabilidad de **escalamiento de privilegios** que afecta a **Microsoft Sharepoint Server** y **Skype for Business** (las versiones específicas afectadas pueden ser visualizadas en el apartado "**Security Updates**" del siguiente enlace), la misma ha sido identificada con el **CVE-2020-1025**. La explotación exitosa de este fallo permitiría a un atacante **escalar privilegios** en el sistema omitiendo la autenticación.

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

- Microsoft JET Database Engine
- Microsoft Graphics Component
- Microsoft Edge
- Azure DevOps
- Internet Explorer
- Microsoft OneDrive
- Microsoft Windows
- Visual Studio

Se detectaron vulnerabilidades de **escalada de privilegios** y **ejecución remota de código** en **Visual Studio** (CVE-2020-1416, CVE-2020-1481), múltiples vulnerabilidades de **elevación de privilegios** y **divulgación de información** en el **kernel de Windows** (CVE-2020-1396, CVE-2020-1336, CVE-2020-1426). Así como también, múltiples vulnerabilidades de **divulgación de información** en **Internet Explorer** y **Microsoft Edge** (CVE-2020-1432, CVE-2020-1433), son algunas de las más resaltantes.

Impacto:

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

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

Solución y prevención:

- Aplicar la actualización de seguridad para el **framework .NET**, **Microsoft Sharepoint** y **Visual Studio** 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**.
- Como medida de mitigación para la vulnerabilidad **SigRed,** se recomienda limitar el tamaño máximo de un mensaje DNS (por TCP) a **0xFF00**, con el siguiente comando:

```
reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters" /v
"TcpReceivePacketSize" /t REG_DWORD /d 0xFF00 /f
net stop DNS && net start DNS
```

Información adicional:

- https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Jul
- https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/
- https://thehackernews.com/2020/07/windows-dns-server-hacking.html