BOLETÍN DE ALERTA

Boletín Nro.: 2020-24

Fecha de publicación: 13/08/2020

Fecha de actualización: 21/08/2020

Tema: Actualizaciones de seguridad en productos de Microsoft abordan 120 vulnerabilidades, 17 de ellas catalogadas como críticas y 103 de riesgo alto.

Las vulnerabilidades catalogadas como **críticas** son: CVE-2020-1554, CVE-2020-1492, CVE-2020-1379, CVE-2020-1477, CVE-2020-1525, CVE-2020-1046, CVE-2020-1472, CVE-2020-1483, CVE-2020-1560, CVE-2020-1339, CVE-2020-1555, CVE-2020-1585, CVE-2020-1568, CVE-2020-1570, CVE-2020-1567, CVE-2020-1380 y CVE-2020-1574.

Productos afectados:

- Microsoft Windows 10, Windows 8.1, Windows 7, Windows Server 2008, Windows Server 2012, Windows Server 2016 y Windows Server 2019
- Microsoft Edge
- Internet Explorer
- Microsoft Scripting Engine
- .NET Framework
- Microsoft Office, Microsoft Office Services y Microsoft Web Apps
- Microsoft Outlook
- Microsoft Windows Codecs Library
- Microsoft Scripting Engine

Descripción:

Recientemente Microsoft ha lanzado actualizaciones de seguridad correspondientes al **Patch Tuesday** de Agosto, las mismas abordan un total de **120 vulnerabilidades** de las cuales **17** han sido catalogadas como **críticas** y **103** de **alto riesgo**. Con dichas actualizaciones se abordaron **2** vulnerabilidades **Zero-Day** activamente explotadas por atacantes. A continuación, se detallan las **17 vulnerabilidades** catalogadas como **críticas**.

Fueron identificadas múltiples vulnerabilidades de **ejecución remota de código**:

Fallos que se dan debido a un procesamiento incorrecto de los **datos de entrada**. El CVE-2020-1046, afecta a **.NET framework** (las versiones específicas afectadas pueden ser visualizadas en el apartado "**Security Updates**" del siguiente enlace). Mientras que el CVE-2020-1567, afecta al **motor de renderizado MSHTML** de **Internet Explorer 9 y 11.**

Por otro lado, múltiples fallos que se dan debido a un mal manejo de objetos en memoria:

- El CVE-2020-1483, afecta a **Microsoft Outlook** (las versiones específicas afectadas pueden ser visualizadas en el apartado "**Security Updates**" del siguiente enlace);
- Los CVE-2020-1560, CVE-2020-1574 y CVE-2020-1585, afectan a la librería **Windows Codecs** de los sistemas **Windows 10** y **Windows Server** (las versiones específicas afectadas pueden ser visualizadas en el apartado "**Security Updates**" del siguiente enlace);
- El CVE-2020-1555, afecta al motor de script de **Microsoft Edge (HTML-based)**;
- El CVE-2020-1568, afecta al lector PDF de **Microsoft Edge (HTML-based)**;
- Los CVE-2020-1570, afecta al motor de script de **Internet Explorer 9 y 11**;
- Los CVE-2020-1554, CVE-2020-1492, CVE-2020-1379, CVE-2020-1477 y CVE-2020-1525, afectan a la plataforma **Media Foundation** de **Windows 10, Windows 8.1, Windows 7, Windows Server 2008, Windows Server 2012** y **Windows Server 2016** (las versiones específicas afectadas pueden ser visualizadas en el apartado "**Security Updates**" del siguiente enlace);
- Finalmente, el CVE-2020-1339, afecta al **códec de audio** de **Windows Media** para los sistemas **Windows 10, WIndows 8, Windows 7, 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).

Además, fue abordada una vulnerabilidad de **escalamiento de privilegios** en el servicio **Netlogon** de los sistemas **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), la misma ha sido identificada con el CVE-2020-1472; y se da cuando un atacante establece una conexión Netlogon vulnerable a un **controlador de dominio,** utilizando el **protocolo remoto de Netlogon** (MS-NRPC). La explotación exitosa de este fallo permitiría a un atacante obtener acceso administrativo y ejecutar **aplicaciones maliciosas** en un equipo de la red.

Vulnerabilidades Zero-Day

Dos de los fallos de seguridad abordados han sido activamente explotados por atacantes sin conocimiento de Microsoft. El CVE-2020-1380 de **riesgo crítico**, trata de una vulnerabilidad de use-after-free que afecta al motor de script de **Internet Explorer 9 y 11;** y se da debido a un mal manejo de objetos en memoria. La explotación exitosa de este fallo permitiría a un atacante **remoto** ejecutar código arbitrario en el contexto del usuario actual. Mientras que el CVE-2020-1464, trata de una vulnerabilidad de Spoofing que afecta a los sistemas **Windows 10, Windows 8, Windows 7, 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 Windows no valida correctamente las **firmas** de archivos. La explotación exitosa de este fallo permitiría a un atacante **local** sobrepasar las características de seguridad y cargar archivos firmados incorrectamente.

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

- Microsoft JET Database Engine
- Microsoft Graphics Component
- Microsoft Edge
- Microsoft Windows
- Visual Studio
- SQL Server
- ASP.NET Core
- Microsoft Dynamics
- Microsoft Office

Se detectaron vulnerabilidades de **ejecución remota de código** y **divulgación de**

información en **Microsoft Office** (CVE-2020-1504, CVE-2020-1495, CVE-2020-1494, CVE-2020-1563, CVE-2020-1583, CVE-2020-1497), múltiples vulnerabilidades de **elevación de privilegios** y **divulgación de información** en el **Kernel de Windows** (CVE-2020-1479, CVE-2020-1417, CVE-2020-1578). Además, una vulnerabilidad de **denegación de servicios (DoS)** en **SQL Server** (CVE-2020-1455), una vulnerabilidad de **ejecución remota de código** en **Visual Studio** (CVE-2020-0604), son algunas de las más resaltantes.

[Actualización 21/08/2020]

El 19 de agosto, de manera complementaria y adicional al anterior anuncio, **Microsoft** informó que los sistemas **Windows 8.1 , Windows RT 8.1 y Windows Server 2012 R2** también estaban afectadas por las vulnerabilidades de **riesgo alto** identificadas con los CVE-2020-1530 y CVE-2020-1537 y lanzó actualizaciones de seguridad de emergencia para abordarlos.

Estos fallos tratan de vulnerabilidades de **elevación de privilegios** en **Windows Remote Access**, que según el anuncio anterior también afectan a **Windows 10, Windows 7, y Windows Server 2008, 2012, 2016, 2019, y Windows Server versiones 1903, 1909, y 2004**.

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 y
- Escalar privilegios.

Solución y prevención:

- Aplicar la actualización de seguridad, desde el apartado "**Security Updates**" de la página oficial de Microsoft, para los siguientes productos:
    - **Internet Explorer 9 y 11**, en el siguiente enlace,
    - **.NET Framework**, en el siguiente enlace,
    - **Microsoft Edge (HTML-Based)**, en el siguiente enlace,

- **Microsoft Outlook**, en el siguiente enlace.

- 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**.
- Aplicar los **parches de seguridad de emergencia** para **Windows 8.1**, **Windows RT 8.1** y **Windows Server 2012 R2**, disponibles desde el siguiente **enlace**.

Información adicional:

- https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Aug
- https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2020-patch-tuesday-fixes-2-zero-days-120-flaws/
- https://thehackernews.com/2020/08/microsoft-software-patches.html
- https://thehackernews.com/2020/08/windows-update-download.html