Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

TETÃ REKUÁI GOBIERNO NACIONAL

BOLETÍN DE ALERTA

Boletín Nro.: 2020-30

Fecha de publicación: 14/10/2020

Tema: Parches para vulnerabilidades críticas en Windows y otros fallos menores.

Microsoft ha publicado actualizaciones de seguridad para varios de sus productos, donde abordan 87 vulnerabilidades, 12 de ellas catalogadas como críticas, 74 como altas y otras de criticidad moderada.

Las vulnerabilidades catalogadas como críticas afectan a los siguientes productos y han sido identificadas como:

1. CVE-2020-16898, **afecta a Windows TCP/IP** en sistemas operativos afectados **con calificación de riesgo 9.8.**
2. CVE-2020-16911, afecta a Windows Graphics Device Interface (GDI) en sistemas operativos afectados, **con calificación de riesgo 8.8**
3. CVE-2020-16891, fallo en Windows Hyper-V en sistemas operativos afectados, **con calificación de riesgo 8.8**
4. CVE-2020-16951, afecta a Microsoft SharePoint, **con calificación de riesgo 8.6**
5. CVE-2020-16952, afecta a Microsoft SharePoint **con calificación de riesgo 8.6**
6. CVE-2020-16947, afecta al software de Microsoft Outlook, **con calificación de riesgo 8.1**
7. CVE-2020-16923, fallo en Microsoft Graphics Components en sistemas operativos afectados, **con calificación de riesgo 7.8**
8. CVE-2020-17003, afecta a Base 3D Viewer, **con calificación de riesgo 7.8**
9. CVE-2020-16967, fallo en Windows Camera Codec Pack en sistemas operativos afectados, **con calificación de riesgo 7.8**
10. CVE-2020-16968, fallo en Windows Camera Codec Pack en sistemas operativos afectados, **con calificación de riesgo 7.8**
11. CVE-2020-16915, fallo en Windows Media Foundation en sistemas operativos afectados, **con calificación de riesgo 7.8**

12. CVE-2020-9746, fallo en Adobe Flash Player, versión 32.0.0.433 y anteriores en: sistemas operativos afectados, **con calificación de riesgo 7**

Descripción:

A continuación se detallan brevemente las **12 vulnerabilidades** de **riesgo crítico** abordadas. **Entre ellas se resalta** la vulnerabilidad de **ejecución remota de código** que afecta a la **pila TCP/IP** de **Windows**, con calificación de riesgo 9.8.

Windows TCP/IP "Bad Neighbor"

La **vulnerabilidad crítica más resaltante**, ha sido identificada con el CVE-2020-16898 y afecta a la **pila TCP/IP** de los sistemas **Windows 10, Windows Server 2019 y Windows Server** (ver versiones específicas afectadas). El fallo se da debido a un manejo incorrecto de paquetes de anuncios del **enrutador ICMPv6**. Un atacante podría explotar exitosamente este fallo enviando **paquetes de anuncios de enrutador ICMPv6 maliciosos** a un **sistema Windows remoto** y de tener éxito **ejecutar código arbitrario** en el servidor o cliente víctima.

Según investigadores de seguridad este fallo podría permitir a atacantes **esparcir un ataque de un sistema vulnerable a otro** sin necesidad de interacción humana.

Se identificaron también múltiples vulnerabilidades de **mal manejo de objetos en memoria**, que permitirían a un atacante **ejecutar código remoto**:

- El CVE-2020-16911 afecta al componente **Windows Graphics Device Interface (GDI)** de los sistemas **Windows 10, Windows 8.1, Windows Server 2012, 2016 y 2019** (ver versiones específicas afectadas). Un atacante podría explotar este fallo de dos formas: En un **escenario basado en web**, el atacante cuenta con un **sitio web malicioso** diseñado especialmente para explotar la vulnerabilidad y convence a un potencial usuario víctima mediante técnicas de ingeniería social para que ingrese al sitio web. En un **escenario basado en archivos compartidos,** un atacante cuenta con un **archivo malicioso** especialmente diseñado para explotar la vulnerabilidad y convence a un potencial usuario víctima para que lo abra.
- El CVE-2020-16947, afecta a **Microsoft Outlook 2016**. Para la explotación exitosa de esta vulnerabilidad es necesario que la víctima abra un **correo electrónico malicioso** especialmente diseñado, en versiones vulnerables de Outlook.

- Mientras que el CVE-2020-16923, afecta al **componente Microsoft Graphics** de los sistemas **Windows 10, Windows 7, Windows 8, Windows Server 2008, 2012, 2016 y 2019** (ver versiones específicas afectadas). Un atacante podría explotar exitosamente este fallo convenciendo a un usuario víctima para que abra un **archivo malicioso** especialmente diseñado.
- El CVE-2020-17003**,** afecta al **motor de renderizado Base3D**. La explotación exitosa podría permitir a un atacante **ejecutar código arbitrario** en el sistema de la víctima.
- Por otro lado, los CVE-2020-16967 y CVE-2020-16968 afectan a **Windows Camera Codec Pack**. Un atacante podría explotar exitosamente este fallo enviando un **archivo malicioso** especialmente diseñado para explotar la vulnerabilidad y ejecutar código arbitrario en el contexto del usuario víctima.
- Finalmente el CVE-2020-16915, afecta a la plataforma **Windows Media Foundation** para **Windows 10, Windows Server 2016, 2019** (ver versiones específicas afectadas). Un atacante podría explotar exitosamente este fallo convenciendo a una potencial víctima para que abra un **archivo malicioso** o visite un **sitio web malicioso**.

Otra de las vulnerabilidades más resaltantes es el CVE-2020-16891 con una calificación de riesgo 8.8, que afecta al programa de virtualización **Windows Hyper-V** para los sistemas **Windows 10, Windows 8.1, Windows 7, Windows Server 2008, 2012, 2016 y 2019** (ver versiones específicas afectadas); y se da debido a que el servidor host no valida correctamente los datos de entrada de un usuario autenticado en un sistema operativo invitado. Un atacante autenticado podría explotar exitosamente este fallo ejecutando una **aplicación maliciosa** especialmente diseñada, en un sistema operativo invitado y de tener éxito **ejecutar código arbitrario** en el **sistema operativo host de Hyper-V.**

El CVE-2020-9746, trata de una vulnerabilidad de tipo NULL Pointer Dereference afecta a **Adobe Flash Player para Microsoft Edge e Internet Explorer 11** en versiones 32.0.0.387 y anteriores para **Windows 10, Windows 8, Windows Server 2012 y 2016** (ver versiones específicas afectadas). La explotación exitosa permitiría a un atacante remoto **ejecutar código arbitrario** en el contexto del usuario víctima.

Los CVE-2020-16951 y CVE-2020-16952, afectan a **Microsoft SharePoint Enterprise**

Server 2016, **Microsoft SharePoint Foundation 2013 Service Pack 1** y **Microsoft SharePoint Server 2019**. Un atacante podría explotar exitosamente este fallo cargando un **paquete de aplicación Sharepoint malicioso** y de tener éxito ejecutar código en el contexto del grupo de aplicaciones Sharepoint.

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;

Solución y prevención:

- Aplicar la actualización de seguridad, desde el apartado "**Security Updates**" de la **página oficial de Microsoft**, para los siguientes productos afectados:
  - **Microsoft Outlook 2016 (32-bit)**, desde el siguiente enlace.
  - **Microsoft Outlook 2016 (64-bit)**, desde el siguiente enlace.
  - **Adobe Flash Player**, desde el siguiente enlace.
  - **Microsoft SharePoint Enterprise Server 2016**, desde el siguiente enlace.
  - **Microsoft SharePoint Foundation 2013**, desde el siguiente enlace.
  - **Microsoft SharePoint Server 2019**, desde el siguiente enlace.
  - **Microsoft .NET Framework**, desde el siguiente enlace.
  - **Visual Studio Code**, 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-Oct
- https://www.bleepingcomputer.com/news/security/microsoft-october-2020-patch-tuesday-fixes-87-security-bugs/
- https://thehackernews.com/2020/10/windows-tcp-ip-patch-tuesday.html