BOLETÍN DE ALERTA

Boletín Nro.: 2020-08
Fecha de publicación: 25/03/2020
Tema: Vulnerabilidades críticas Zero-Day en Windows permiten la ejecución remota de código.

Sistemas afectados:

- Windows 10, en todas las versiones;
- Windows 8.1, en arquitecturas de 32 y 64 bits;
- Windows RT 8.1;
- Windows 7 Service pack 1, en arquitecturas de 32 y 64 bits;
- Windows Server 2008 Service pack 2, Server Core installation, en sus arquitecturas de 32 y 64 bits;
- Windows Server 2012 y Server Core installation;
- Windows Server 2012 R2 y Server Core installation;
- Windows Server 2016 y Server Core installation;
- Windows Server 2019 y Server Core installation.

Descripción:

Recientemente Microsoft ha lanzado un aviso de seguridad, donde informa sobre dos vulnerabilidades críticas **Zero-Day** que están siendo utilizadas por los atacantes para realizar ataques dirigidos. Según el aviso de seguridad, estos **Zero-Day** se dan debido a que la biblioteca **Adobe Type Manager (atmfd.dll)** procesa de manera insegura ciertos tipos de fuentes en formato **Adobe Type 1 PostScript**, lo que permitirían a un atacante ejecutar código malicioso en el contexto del usuario actual.

La Biblioteca **Adobe Type Manager** de Windows, permite el análisis de fuentes que no solo analiza el contenido cuando se abre con un software de terceros, sino que también lo utiliza el Explorador de Windows para mostrar el contenido de un archivo en el **"Panel de vista previa"** o el **"Panel de detalles"** sin que los usuarios lo abran, por lo que la explotación de esta vulnerabilidad se puede dar de varias maneras, por ejemplo un atacante podría convencer a un

usuario para que abra un documento especialmente diseñado, o lo vea en el **"Panel de vista previa"** de Windows.

El aviso de seguridad de Microsoft, además informa que el parche que aborda estos fallos no estaría disponible hasta el **"Patch tuesday"** del 14 de abril, por lo que recomienda a usuarios y empresas aplicar las medidas de mitigación.

Impacto:

Estas vulnerabilidades podrían permitir a un atacante remoto ejecutar código malicioso en el contexto del usuario actual, pudiendo obtener el control total del sistema operativo afectado.

Solución y prevención:

Con la aplicación de una de las siguientes medidas citadas a continuación, se podrá mitigar las vulnerabilidades:

1. Deshabilite el **Panel de vista previa** y **el Panel de detalles** en el Explorador de Windows:

    a. Para deshabilitar estos paneles en **Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 y Windows 8.1**, realice los siguientes pasos:

    - Abra el Explorador de Windows, haga clic en **Organizar** y luego en **Diseño**.
    - Desactive las opciones de menú del **Panel de detalles** y del **Panel vista previa**.
    - Haga clic en **Organizar** y luego en **Carpeta y opciones de búsqueda**.
    - Haga clic en la pestaña **Ver**.
    - En Configuración avanzada, marque la casilla **Mostrar siempre iconos, nunca miniaturas**.
    - Cierre todas las instancias abiertas del Explorador de Windows para que el cambio surja efecto.

b. Para **Windows Server 2016, Windows 10 y Windows Server 2019**, realice los siguientes pasos:

- Abra el Explorador de Windows, haga clic en la pestaña **Ver**.
- Desactive las opciones de menú del **Panel de detalles** y del **Panel vista previa**.
- Haga clic en **Opciones** y luego en **Cambiar carpeta y opciones de búsqueda**.
- Haga clic en la pestaña **Ver**.
- En Configuración avanzada, marque la casilla **Mostrar siempre iconos, nunca miniaturas**.
- Cierre todas las instancias abiertas del Explorador de Windows para que el cambio surja efecto.

2. Deshabilitar el servicio **WebClient**, para ello realice los siguientes pasos:

- Haga clic en Inicio, y busque **Ejecutar** (o presione la tecla de **Windows + R**), escriba **Services.msc** y luego haga clic en **Aceptar**.
- Haga clic con el botón derecho en el servicio **WebClient** y seleccione **Propiedades**.
- Cambie el tipo de Inicio a **Deshabilitado**. Si el servicio se está ejecutando, haga clic en **Detener** antes de deshabilitarlo.
- Haga clic en **Aceptar** y salga de la aplicación de administración.

3. Renombrar o deshabilitar **ATMFD.DLL**, para ello ingrese los siguientes comandos en el símbolo del sistema **(CMD)** con permisos administrativos:

a. Para sistemas de 32 bits:

- cd "%windir%\system32"

- takeown.exe /f atmfd.dll
- icacls.exe atmfd.dll /save atmfd.dll.acl
- icacls.exe atmfd.dll /grant Administrators:(F)
- rename atmfd.dll x-atmfd.dll
- Reinicie su equipo.

b. Para sistemas de 64 bits:

- cd "%windir%\system32"
- takeown.exe /f atmfd.dll
- icacls.exe atmfd.dll /save atmfd.dll.acl
- icacls.exe atmfd.dll /grant Administrators:(F)
- rename atmfd.dll x-atmfd.dll
- cd "%windir%\syswow64"
- takeown.exe /f atmfd.dll
- icacls.exe atmfd.dll /save atmfd.dll.acl
- icacls.exe atmfd.dll /grant Administrators:(F)
- rename atmfd.dll x-atmfd.dll
- Reinicie su equipo.

Información adicional:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200006
- https://www.zdnet.com/article/microsoft-warns-of-windows-zero-day-exploited-in-the-wild/
- https://thehackernews.com/2020/03/windows-adobe-font-vulnerability.html
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/vulnerabilidades-ejecucion-remota-codigo-microsoft-windows