Microsoft emitió este lunes un nuevo aviso de seguridad que advierte a miles de millones de usuarios de Windows sobre dos nuevas vulnerabilidades críticas de día cero sin parches, que podrían permitir a los hackers tomar el control total de las computadoras de forma remota.

Según Microsoft, las dos vulnerabilidades se están explotando en ataques limitados y dirigidos que impactar a todas las versiones compatibles del sistema operativo Windows, incluyendo las ediciones Windows 10, 8.1 y Server 2008, 2012, 2016 y 2019, además de Windows 7, para las cuales Microsoft finalizó su soporte el 14 de enero de 2020.

Las dos vulnerabilidades residen en la Biblioteca Adobe Type Manager de Windows, un software de 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.

Las fallas se presentan en Microsoft Windows cuando la biblioteca Adobe Type Manager Library *«maneja incorrectamente una fuente multimaestro especialmente diseñada – formato Adobe Type 1 PostScript»,* lo que permite a los atacantes remotos ejecutar código malicioso arbitrario en sistemas específicos al convencer a un usuario de abrir un documento elaborado o verlo en el panel Vista previa de Windows.

> *«Para los sistemas que ejecutan versiones compatibles de Windows 10, un ataque exitoso solo podría resultar en la ejecución de código dentro de un contexto de sandbox AppContainer con capacidades y privilegios limitados»,* dijo Microsoft.

Hasta el momento, no está claro si los defectos también pueden activarse remotamente por medio de un navegador web al convencer a un usuario de visitar una página web que contenga fuentes OTF maliciosas especialmente diseñadas. Existen muchas otras formas en que un atacante podría explotar la vulnerabilidad, por ejemplo, por medio del servicio de cliente de creación y control de versiones distribuidas web (WebDAV).

Microsoft asegura estar al tanto del problema y está trabajando en un parche, que la compañía lanzará a todos los usuarios de Windows como parte de sus próximas actualizaciones Patch Tuesday, el 14 de abril.

> *«La configuración de seguridad mejorada no mitiga esta vulnerabilidad»,* dice la compañía.

Mientras tanto, es posible aplicar algunas soluciones alternativas:

Deshabilitar el panel de vista previa y el panel de detalles en el Explorador de Windows

Para deshabilitar la función de panel de vista previa y panel de detalles, puedes seguir los siguientes pasos:

1.- Abrir el explorador de Windows, hacer clic en Organizar y en Diseño.
2.- Desactivar las opciones de menú del panel Detalles y del panel Vista previa.
3.- Hacer clic en organizar y en Carpeta, después en opciones de búsqueda.
4.- Hacer clic en la pestaña Ver.
5.- En configuración avanzada, marcar la casilla Mostrar siempre iconos, nunca miniaturas.
6.- Cerrar todas las instancias abiertas del Explorador de Windows para que el cambio surta efecto.

Debe tenerse en cuenta que aunque esta solución evita que se vean archivos maliciosos en el Explorador de Windows, no es estricto que ningún software legítimo de terceros cargue la biblioteca de análisis de fuentes vulnerables.

Deshabilitar el servicio WebClient

Además, también se recomienda deshabilitar el servicio WebClient de Windows para evitar ataques cibernéticos por medio del servicio de cliente WebDAV.

1.- Hacer clic en Inicio, Ejecutar (o presionar Windows+R), escribir services.msc y dar clic en Aceptar.
2.- Hacer clic con el botón derecho en el servicio WebClient y seleccionar Propiedades.
3.- Cambiar el tipo de Inicio a Deshabilitado. Si el servicio se está ejecutando, hacer clic en Detener.
4.- Hacer clic en Aceptar y salir de la aplicación de administración.

> *«Después de aplicar esta solución alternativa, sigue siendo posible que los atacantes remotos que exploten con éxito esta vulnerabilidad hagan que el sistema ejecute programas ubicados en la computadora del usuario objetivo o en la Red de Área Local (LAN), pero se solicitará a los usuarios que confirmen antes de abrir de forma arbitraria programas de Internet»,* dijo Microsoft.

Renombrar o deshabilitar ATMFD.dll

Microsoft también recomienda a los usuarios a cambiar el nombre del archivo Adobe Type Manager Font Driver (ATMFD.dll) para deshabilitar temporalmente la tecnología de fuente incorporada, lo que podría causar que ciertas aplicaciones de terceros dejen de funcionar.

Es necesario ingresar los siguientes comandos en un símbolo del sistema administrativo:

Para 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

Para 64 bits:

cd «%windir%\system32»
takeown.exe /f atmfd.dll
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

Reiniciar el sistema.