BOLETÍN DE ALERTA

Boletín Nro.: 2021-39

Fecha de publicación: 17/12/2021

Tema: Microsoft publica parches para múltiples vulnerabilidades

Software y sistemas operativos afectados:

- Microsoft Windows 8, 8.1 y 10.
- Microsoft Windows Server 2012, 2016 y 2019.
- Microsoft Office
- Microsoft Powershell
- Microsoft Edge
- Kernel de Windows
- Cola de impresión de Windows
- Escritorio remoto de Windows

Para visualizar la lista detallada de los productos afectados ingrese al siguiente enlace: https://msrc.microsoft.com/update-guide/deployments

Descripción:

Microsoft ha publicado 67 correcciones de seguridad de múltiples de sus productos, entre las cuales 7 corresponden a vulnerabilidades de día cero (*Zero Day*). Entre los tipos de vulnerabilidades parchadas más críticas se encuentran las siguientes:

- Ejecución remota de comando
- Escalamiento de privilegios
- Denegación de servicio

Las vulnerabilidades críticas parchadas son:

CVE-2021-43890 de severidad alta con una puntuación de 7.2, se debe a una falla en un componente de la estructura de archivo *appX* de Windows, lo que permitiría a un atacante realizar denegación de servicio para luego derivar en ejecución remota de comandos. Microsoft advierte sobre la explotación activa de esta vulnerabilidad a través del diseño de paquetes malintencionados que incluyen los malwares conocidos como Emotet, Trickbot y Bazaloader".

CVE-2021-42310 de severidad alta con una puntuación de 8.1, se debe a una validación de entrada incorrecta en Microsoft Defender para IoT, lo que permitiría a un atacante remoto enviar una solicitud maliciosamente diseñada con el objetivo de realizar ejecución remota de código en el sistema afectado.

CVE-2021-43240 de severidad alta con una puntuación de 7.0, se debe a una falla en la función *SetFileShortNameA* de la librería *Winbase.h,* que permitiría a un atacante escalar privilegios en el sistema afectado.

CVE-2021-43880 de severidad alta (aún sin puntuación asignada), se debe a una falla en el componente *Mobile Device Management* de Windows, que permitiría a un atacante realizar escalamiento de privilegios en el sistema afectado.

CVE-2021-43883 de severidad alta, con una puntuación de 7.8. Se debe a una falla en un componente de *Windows Installer,* que permitiría a un atacante realizar escalamiento de privilegios en el sistema afectado.

CVE-2021-43893 de severidad media con una puntuación de 6.5, se debe a una falla de las restricciones de seguridad en el sistema de cifrado de archivos (EFS) de Windows, que permitiría a un atacante realizar un escalamiento de privilegios en el sistema afectado.

CVE-2021-41333 de severidad alta con una puntuación de 7.8, se debe a una falla en una función del componente *Print Spooler* esto permitiría a un atacante realizar escalamiento de privilegios en el sistema afectado.

Impacto:

La explotación exitosa de estas vulnerabilidades podría comprometer el sistema vulnerable.

Solución:

Se recomienda actualizar a la versión más reciente el software o sistema operativo afectado correspondiente, de acuerdo a los siguientes enlaces:

- https://docs.microsoft.com/en-us/officeupdates/update-history-office-2019
- https://support.microsoft.com/en-us/windows/get-the-latest-windows-update-7d20e88c-0568-483a-37bc-c3885390d212#WindowsVersion=Windows_10

Información adicional:

- https://docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-setfileshortnamea
- https://msrc.microsoft.com/update-guide/