OPENLINK

SISTEMAS DE REDES DE DATOS

Vulnerabilidad de elevación de privilegios en Windows

Existe una vulnerabilidad de elevación de privilegios en Windows cuando el componente Win32k no procesa correctamente los objetos en la memoria, de tipo Use-After-Free. La explotación de la vulnerabilidad permite al malware descargar y ejecutar un script desarrollado por los atacantes que puede lograr el control del ordenador infectado.

Windows®

Impacto de la vulnerabilidad	Severidad	CVE	CVSS 3
Control total del sistema	Alta	CVE-2019-0859	7.8 HIGH

Información sobre el sistema/producto afectado

Los productos afectados por esta vulnerabilidad son los siguientes:

- **Microsoft Windows Server 2019**
- **Microsoft Windows Server 2016**
- **Microsoft Windows Server 2012**
- **Microsoft Windows Server 2008**
- **Microsoft Windows 8.1**
- **Microsoft Windows 7**
- **Microsoft Windows 10**

Para conocer con más detalle si su versión es afectada por esta vulnerabilidad por favor consulte el siguiente enlace:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0859

¿Cómo determinar si tenemos alguna de estas versiones afectadas?

Para determinar si es afectado por esta vulnerabilidad, es suficiente con verificar la versión del sistema operativo Windows, puede validar esta información ingresando a una ventana de Shell de comando MS-DOS de Microsoft "cmd" y escribir el comando #winver, presionar la tecla "Enter" para ejecutar el comando y posteriormente se mostrará la información sobre su versión de Windows, para mayor información consulte: https://support.microsoft.com/en-us/help/13443/windows-which-operating-system

¿Qué impacto tendría si la vulnerabilidad es explotada?

Aprovechando este fallo de seguridad, un atacante podría tomar control total del servidor, comprometiendo la integridad, confidencialidad y disponibilidad del sistema.

Fuente

https://latam.kaspersky.com/blog/cve-2019-0859-detected/14382/

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0859

https://securelist.com/new-win32k-zero-day-cve-2019-0859/90435/

¿Qué hacer si tenemos la vulnerabilidad?

Windows ha dispuesto una actualización de seguridad la cual mitiga esta vulnerabilidad. La versión se puede descargar directamente de la web de Microsoft: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0859

Antes de realizar el upgrade verifique con su administrador la compatibilidad de la nueva versión con las aplicaciones y hardware existentes en su compañía.

SI DETECTA ALGÚN EVENTO DE ESTE TIPO EN SU RED, NO DUDE EN PONERSE EN CONTACTO CON EL NOC/SOC DE OPENLINK:

soc@oplk.com
mercadeo@oplk.com
+58 212 273 4300 Op. 1-2
+57 1 432 1740 Ext. 574430
+1 787 273 0876