Alerta de seguridad cibernética	9VSA20-00256-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Muy Alto
TLP	Blanco
Fecha de lanzamiento original	1 de julio de 2020
Última revisión	1 de julio de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de Microsoft referente a dos vulnerabilidades, una crítica y otra importante, las que afectan a la Biblioteca de Codecs (colección de bibliotecas de soporte que ayudan al sistema operativo Windows a reproducir, comprimir y descomprimir varias extensiones de archivos de audio y video) de Windows, un vector de ataque que pude ser explotado a través de ingeniería social al ejecutar archivos multimedia maliciosos.

Vulnerabilidades

CVE-2020-1425
CVE-2020-1457

CVE-2020-1425

Existe una vulnerabilidad de ejecución remota de código en la forma en que la Biblioteca de Codecs de Microsoft Windows trata los objetos en la memoria. Un atacante que explotara con éxito esta vulnerabilidad podría obtener información para comprometer el sistema del usuario. La explotación de la vulnerabilidad requiere que un programa procese un archivo de imagen especialmente diseñado. La actualización corrige la vulnerabilidad al corregir cómo Microsoft Windows Codecs Library maneja los objetos en la memoria.

Productos Afectados

Windows 10
Server

Mitigación para Windows 10

Windows 10 versión 1709 para sistemas de 32 bits
Windows 10 versión 1709 para sistemas basados en ARM64
Windows 10 versión 1709 para sistemas x64
Windows 10 versión 1803 para sistemas de 32 bits
Windows 10 versión 1803 para sistemas basados en ARM64
Windows 10 versión 1803 para sistemas basados en x64
Windows 10 versión 1809 para sistemas de 32 bits
Windows 10 versión 1809 para sistemas basados en ARM64
Windows 10 versión 1809 para sistemas x64
Windows 10 versión 1903 para sistemas de 32 bits
Windows 10 versión 1903 para sistemas basados en ARM64
Windows 10 versión 1903 para sistemas x64
Windows 10 versión 1909 para sistemas de 32 bits
Windows 10 versión 1909 para sistemas basados en ARM64
Windows 10 versión 1909 para sistemas x64
Windows 10 versión 2004 para sistemas de 32 bits
Windows 10 versión 2004 para sistemas basados en ARM64
Windows 10 versión 2004 para sistemas x64

Mitigación para Server

Windows Server 2019
Windows Server 2019 (instalación de Server Core)
Windows Server, versión 1803 (instalación de Server Core)
Windows Server, versión 1903 (instalación Server Core)
Windows Server, versión 1909 (instalación Server Core)
Windows Server, versión 2004 (instalación Server Core)

Enlaces

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-1425
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1425

CVE-2020-1457

Existe una vulnerabilidad de ejecución remota de código en la forma en que la Biblioteca de Codecs de Microsoft Windows trata los objetos en la memoria. Un atacante que explotara con éxito la vulnerabilidad podría ejecutar código arbitrario. La explotación de la vulnerabilidad requiere que un programa procese un archivo de imagen especialmente diseñado. La actualización corrige la vulnerabilidad al corregir cómo Microsoft Windows Codecs Library maneja los objetos en la memoria.

Productos Afectados

Windows 10
Server

Mitigación para Windows 10

Windows 10 versión 1709 para sistemas de 32 bits
Windows 10 versión 1709 para sistemas basados en ARM64
Windows 10 versión 1709 para sistemas x64
Windows 10 versión 1803 para sistemas de 32 bits
Windows 10 versión 1803 para sistemas basados en ARM64
Windows 10 versión 1803 para sistemas basados en x64
Windows 10 versión 1809 para sistemas de 32 bits
Windows 10 versión 1809 para sistemas basados en ARM64
Windows 10 versión 1809 para sistemas x64
Windows 10 versión 1903 para sistemas de 32 bits
Windows 10 versión 1903 para sistemas basados en ARM64
Windows 10 versión 1903 para sistemas x64
Windows 10 versión 1909 para sistemas de 32 bits
Windows 10 versión 1909 para sistemas basados en ARM64
Windows 10 versión 1909 para sistemas x64
Windows 10 versión 2004 para sistemas de 32 bits
Windows 10 versión 2004 para sistemas basados en ARM64
Windows 10 versión 2004 para sistemas x64

Mitigación para Server

Windows Server 2019
Windows Server 2019 (instalación de Server Core)
Windows Server, versión 1709 (instalación de Server Core)
Windows Server, versión 1903 (instalación Server Core)
Windows Server, versión 2004 (instalación Server Core)

Enlaces

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-1457
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1457