Alerta de seguridad cibernética	9VSA20-00309-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de octubre de 2020
Última revisión	22 de octubre 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 respecto a dos vulnerabilidades que afectan a la ejecución de código remoto (RCE) corregidos en la biblioteca de códecs de Windows y Visual Studio Code. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-17022
CVE-2020-17023

CVE-2020-17022

Un atacante pueden crear imágenes maliciosas que, cuando son procesadas por una aplicación que se ejecuta en Windows, pueden permitir que el atacante ejecute código en un sistema operativo Windows sin parches. La explotación de la vulnerabilidad requiere que un programa procese un archivo de imagen especialmente diseñado.

Productos Afectados

Windows 10 versión 1709 para sistemas 32-bit
Windows 10 versión 1709 para sistemas ARM64-based
Windows 10 versión 1709 para sistemas x64-based
Windows 10 versión 1803 para sistemas 32-bit
Windows 10 versión 1803 para sistemas ARM64-based
Windows 10 versión 1803 para sistemas x64-based
Windows 10 versión 1809 para sistemas 32-bit
Windows 10 versión 1809 para sistemas ARM64-based
Windows 10 versión 1809 para sistemas x64-based
Windows 10 versión 1903 para sistemas 32-bit
Windows 10 versión 1903 para sistemas ARM64-based
Windows 10 versión 1903 para sistemas x64-based
Windows 10 versión 1909 para sistemas ARM64-based
Windows 10 versión 1909 para sistemas x64-based
Windows 10 versión 2004 para sistemas 32-bit
Windows 10 versión 2004 para sistemas ARM64-based
Windows 10 versión 2004 para sistemas x64-based

Mitigación

La actualización corrige la vulnerabilidad al corregir cómo la biblioteca de códecs de Microsoft Windows maneja los objetos en la memoria. Se debe actualizar a la última versión de Windows 10 para subsanar la vulnerabilidad.

Enlaces

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17022

CVE-2020-17023

Existe una vulnerabilidad de ejecución de código remoto en Visual Studio Code, en la que se engaña a un usuario para que abra un archivo "package.json" malicioso. El atacante explota la vulnerabilidad ejecutando código arbitrario en el contexto del usuario actual. Si el usuario actual está conectado con privilegios de administrador, el atacante podría tomar el control del sistema afectado. El atacante podría instalar programas; ver, cambiar o eliminar datos; crear nuevas cuentas con privilegios de administrador. Para aprovechar esta vulnerabilidad, el atacante necesitaría convencer a una víctima de que clone un repositorio y lo abra en Visual Studio Code.

Productos Afectados

Visual Code Studio versiones anteriores a la 1.50.1.

Mitigación

La actualización corrige la vulnerabilidad al modificar la forma en que Visual Studio Code maneja los archivos JSON en la versión 1.50.1 de Visual Studio Code.

Enlaces

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17023