Para el primer martes de parches de Microsoft de 2021, la compañía lanzó actualizaciones de seguridad que abordan un total de 83 fallas que abarcan hasta 11 productos y servicios, incluyendo una vulnerabilidad de día cero explotada activamente.

Los últimos parches de seguridad cubren Microsoft Windows, el navegador Edge, ChakraCore, Office y Microsoft Office Services, Web Apps, Visual Studio, Microsoft Malware Engine, .NET Core, ASP .NET y Azure. De las 83 vulnerabilidades, 10 son críticas y 73 importantes en gravedad.

El más grave de los problemas es una falla de ejecución remota de código (RCE) en Microsoft Defender (CVE-2021-1647), que podría permitir a los atacantes infectar sistemas específicos con código arbitrario.

Microsoft Malware Protection Engine (mpengine.dll) proporciona las capacidades de análisis, detección y limpieza para el software antivirus y antispyware Microsoft Defender. La última versión del software afectada por la falla es 1.1.17600.5, antes de que se abordara en la versión 1.1.17700.4.

Además, se sabe que el error ha sido explotado activamente en la naturaleza, aunque los desatalles no son muchos referentes a qué tan generalizados están los ataques o cómo se explota. También es una vulnerabilidad de cero clic, ya que el sistema vulnerable puede explotarse sin ninguna interacción del usuario.

Microsoft dijo que a pesar de la explotación activa, la técnica no es funcional en todas las situaciones y que aún se considera que el exploit está en un nivel de prueba de concepto, con modificaciones sustanciales necesarias para que funcione de forma eficaz.

Posiblemente la falla ya se haya resuelto como parte de las actualizaciones automáticas del motor de protección contra malware, que generalmente se publica una vez al mes o cuando es necesario para protegerse contra amenazas recién descubiertas, a menos que los sistemas no estén conectados a Internet.

> *«Para las organizaciones que están configuradas para la actualización automática, no se deberían requerir acciones, pero una de las primeras acciones que un actor de amenazas o malware intentará es interrumpir la protección contra amenazas en un sistema para bloquear las actualizaciones de definición y motor»*, dijo Chris Goettl, director senior de gestión de productos y seguridad de Ivanti.

El martes de parches también corrige una falla de escalada de privilegios (CVE-2021-1648) introducida por un parche anterior en la API GDI Print/Print Spooler («splwow64.exe») que fue revelado por Google Project Zero el mes pasado después de que Microsoft no lo arregló dentro de los 90 días posteriores a la divulgación responsable el 24 de septiembre de 2020.

Otras vulnerabilidades solucionadas por Microsoft incluyen vulnerabilidades de corrupción de memoria en el navegador Microsoft Edge (CVE-2021-1705), una falla de omisión de la característica de seguridad principal del Protocolo de escritorio remoto de Windows (CVE-2021-1674) y cinco vulnerabilidades críticas de RCE en Tiempo de Ejecución de Llamada a Procedimiento Remoto.