Microsoft lanza parches para 112 vulnerabilidades en sus productos

Autor: I. Stepanenko

Fecha: Friday 27th of November 2020 05:01:24 AM

Microsoft lanzó correcciones para 112 vulnerabilidades de seguridad recién descubiertas, como parte del martes de parches de noviembre de 2020. Entre las vulnerabilidades corregidas, se encuentra una falla de día cero explotada activamente que el equipo de seguridad de Google reveló la semana pasada.

17 de las vulnerabilidades abordadas están calificadas como críticas, 93 como importantes y dos tienen una gravedad baja, lo que eleva el recuento de parches a más de 110 luego de una caída el mes pasado.

Las actualizaciones de seguridad abarcan una gama de software, incluidos Microsoft Windows, Office y Office Services, Web Apps, Internet Explorer, Edge, ChakraCore, Exchange

Server, Microsoft Dynamics, Windows Codecs Library, Azure Sphere, Windows Defender, Microsoft Teams y Visual Studio.

Una de las vulnerabilidades de importancia es CVE-2020-17087, con puntuación CVSS de 7.8, que es una falla de desbordamiento de búfer en el controlador de criptografía del kernel de Windows «*cng.sys*«, que fue revelada el 30 de octubre por el equipo de Google Project Zero, utilizado junto con un 0-day de Chrome para comprometer a los usuarios de Windows 7 y Windows 10.

Por su parte, Google lanzó una actualización para su navegador Chrome para abordar el día cero CVE-2020-15999 el mes pasado.

El aviso de Microsoft sobre la falla no menciona más detalles a parte de que se trata de una *«vulnerabilidad local de elevación de privilegios del kernel de Windows»*, en parte para reestructurar los avisos de seguridad en línea con el formato del Common Vulnerability Scoring System (CVSS) a partir de este mes.

Aparte del día cero, la actualización corrige una serie de vulnerabilidades de ejecución remota de código (RCE) que afectan a Exchange Server (CVE-2020-17084), Network File System (CVE-2020-17051) y Microsoft Teams (CVE-2020-17091), así como una falla de seguridad en el software de virtualización Windows Hyper-V (CVE-2020-17040).

CVE-2020-17051 tiene una calificación de 9.8 de un máximo de 10 en la puntuación CVSS, lo que la convierte en una vulnerabilidad crítica. Sin embargo, Microsoft dijo que la complejidad del ataque de la falla es baja debido a las condiciones más allá del control de atacante que deben existir para explotar la vulnerabilidad.

Al igual que con el día cero, los avisos asociados con estas deficiencias de seguridad tienen pocas descripciones sobre cómo se pueden abusar las vulnerabilidades.

Otras fallas críticas corregidas por Microsoft este mes, incluyen vulnerabilidades de corrupción de memoria en Microsoft Scripting Engine (CVE-2020-17052) e Internet Explorer (CVE-2020-17053), además de múltiples fallas de RCE en la biblioteca de códecs de

extensiones de video HEVC.