Microsoft lanzó parches para 79 vulnerabilidades, incluyendo 3 del sistema operativo Windows que están siendo explotadas activamente

El martes, Microsoft informó sobre tres nuevas fallas de seguridad que afectan la plataforma Windows y que están siendo activamente explotadas, como parte de su actualización Patch Tuesday de septiembre de 2024.

Este lanzamiento mensual de seguridad corrige un total de 79 vulnerabilidades, de las cuales siete se califican como críticas, 71 se consideran importantes y una es moderada en términos de gravedad. Además, se solucionaron 26 vulnerabilidades en el navegador Edge, basado en Chromium, desde la actualización Patch Tuesday del mes anterior.

Las tres fallas que han sido explotadas en un contexto malicioso se enumeran a continuación, junto con una vulnerabilidad que Microsoft ha considerado explotada:

- CVE-2024-38014 (Puntuación CVSS: 7.8): Vulnerabilidad de elevación de privilegios en Windows Installer.
- CVE-2024-38217 (Puntuación CVSS: 5.4): Vulnerabilidad de omisión de la característica de seguridad «Marca de la Web» (MotW) en Windows.
- CVE-2024-38226 (Puntuación CVSS: 7.3): Vulnerabilidad de omisión de la característica de seguridad en Microsoft Publisher.
- CVE-2024-43491 (Puntuación CVSS: 9.8): Vulnerabilidad de ejecución remota de código en Windows Update.

> *«La explotación de CVE-2024-38226 y CVE-2024-38217 puede permitir la omisión de funciones de seguridad clave que impiden la ejecución de macros en Microsoft Office»,* explicó Satnam Narang, ingeniero de investigación senior en Tenable.
>
> *«En ambos casos, la víctima debe ser inducida a abrir un archivo manipulado desde un servidor controlado por el atacante. La diferencia es que, para la CVE-2024-38226, el atacante necesita estar autenticado en el sistema y tener acceso local para explotarla».*

Elastic Security Labs reveló el mes pasado que la CVE-2024-38217, también conocida como *LNK Stomping*, ha sido utilizada en ataques desde febrero de 2018.

Por otro lado, la CVE-2024-43491 es significativa por su similitud con un ataque de degradación que la empresa de ciberseguridad SafeBreach detalló a principios del mes pasado.

> *«Microsoft está al tanto de una vulnerabilidad en el Servicing Stack que revirtió algunas correcciones de fallos en componentes opcionales de Windows 10, versión 1507 (lanzada en julio de 2015)»,* señaló la compañía.

«Esto significa que un atacante podría explotar estas vulnerabilidades previamente mitigadas en sistemas con Windows 10, versión 1507 (Windows 10 Enterprise 2015 LTSB y Windows 10 IoT Enterprise 2015 LTSB) que hayan instalado la actualización de seguridad de marzo de 2024 — KB5035858 (OS Build 10240.20526) u otras actualizaciones lanzadas hasta agosto de 2024».

Microsoft también indicó que este problema puede resolverse instalando la actualización de *Servicing Stack* de septiembre de 2024 (SSU KB5043936) y la actualización de seguridad de Windows de septiembre de 2024 (KB5043083), en ese orden.

Es relevante destacar que la evaluación de *«Explotación Detectada»* para la CVE-2024-43491 se debe a la reversión de las correcciones que solucionaban vulnerabilidades en componentes opcionales de Windows 10 (versión 1507) que ya habían sido explotadas.

> *«No se ha detectado explotación directa de la CVE-2024-43491. Además, el equipo de producto de Windows descubrió este problema y no hay evidencia de que sea conocido públicamente»,* dijo Microsoft.