Google Chrome lanzó una actualización de emergencia el día primero de noviembre, que debes instalar inmediatamente para los sistemas Windows, Mac y Linux.

Con Chrome 78.0.3904.87, Google advierte a millones de usuarios que instalen la actualización inmediatamente para parchear dos vulnerabilidades graves, una de estas, está siendo explotada para secuestrar computadoras.

El equipo de seguridad del navegador Chrome no reveló detalles técnicos acerca de la vulnerabilidad, sólo informó que ambos problemas son vulnerabilidades sin uso, uno afecta el componente de audio de Chrome (CVE-2019-13720), mientras que el otro reside en la biblioteca PDFium (CVE-2019-13721).

La vulnerabilidad de uso libre posterior es una clase de problema de corrupción de memoria que permite la corrupción o modificación de datos en la memoria, permitiendo así a un usuario sin privilegios escalar estos en un sistema o software afectado.

Por lo tanto, ambos defectos podrían permitir a los atacantes remotos obtener privilegios en el navegador web Chrome, con el simple hecho de convencer a los usuarios específicos de que visiten un sitio web malicioso, lo que les permite escapar de las protecciones de sandbox y ejecutar código malicioso arbitrario en los sistemas objetivo.

Vulnerabilidad Zero-Day en Chrome se encuentra bajo ataques activos

Descubierto e informado por los investigadores de Kaspersy, Anton Ivanov y Alexey Kulaev, el problema del componente de audio en la aplicación Chrome, se descubrió siendo explotado en la naturaleza, aunque en este momento no está claro qué grupo específico de hackers lo está haciendo.

> *«Google está al tanto de los informes de que existe un exploit para CVE-2019-13720 en la naturaleza. El acceso a los detalles y enlaces de los errores puede mantenerse restringido hasta que la mayoría de los usuarios se actualicen*

> *con una solución. También conservamos las restricciones si el error existe en una biblioteca de terceros de la que dependen otros proyectos de forma similar, pero que aún no se han solucionado»*, dijo el equipo de seguridad de Google Chrome en una publicación.

El problema de uso libre es una de las vulnerabilidades más comunes descubiertas y parcheadas en el navegador web Chrome en los últimos meses.

Hace más de un mes, Google lanzó una actualización de seguridad urgente para Chrome para parchear un total de cuatro vulnerabilidades sin uso en distintos componentes del navegador web, la más grave, podría permitir a los hackers remotos tomar el control del sistema afectado.

En marzo de este año, Google también lanzó una actualización de seguridad de emergencia para Chrome, luego de que se descubriera que los delincuentes explotaban activamente una vulnerabilidad de día cero de Chrome sin uso similar en la naturaleza que afecta el componente FileReader del navegador.

Detalles del exploit 0-Day

Un día después de que Google lanzó una actualización de parche de emergencia para el navegador Chrome para corregir dos vulnerabilidades de alta gravedad, la compañía de seguridad cibernética Kaspersky Labs, reveló más detalles técnicos sobre los que informó a Google y fueron descubiertas siendo explotadas en la naturaleza.

Según los investigadores, los hackers comprometieron un portal de noticias coreano. Plantaron el código de explotación en el sitio, como un pozo de agua, para hackear las computadoras de sus visitantes que abren el portal de noticias utilizando versiones vulnerables de Google Chrome.

Los informes mencionan que el exploit instala el malware de primera etapa en los sistemas de destino luego de explotar la vulnerabilidad de Chrome CVE-2019-13720, que luego se conecta a un servidor de control y comando remoto codificado para descargar la carga útil final.

Operation WizardOpium es el nombre que los investigadores dieron al ataque cibernético, que aún no se ha atribuido a ningún grupo específico de hackers. Sin embargo, los investigadores encontraron algunas similitudes en el código de explotación con el grupo de hackers Lazarus.

> *«Hasta ahora, no hemos podido establecer un vínculo definitivo con ningún actor de amenaza conocido. Existen ciertas similitudes de código muy débiles con los ataques de Lazarus, aunque bien podrían ser una bandera falsa. El perfil del sitio web objetivo está más en línea con los ataques anteriores de DarkHotel que recientemente desplegaron ataques similares de falsa bandera»,* dijo Kaspersky.

Puedes obtener más detalles sobre Operation WizardOpium, que explota la vulnerabilidad de Chrome, en el nuevo informe que publicó Kaspersky.

Parche disponible para Google Chrome

Para parchear las dos vulnerabilidades, Google ya comenzó a implementar la versión 78.0.3904.87 de Chrome para los sistemas operativos Windows, Mac y Linux.

Aunque Chrome notifica de forma automática a los usuarios sobre las actualizaciones disponibles, es recomendable que los usuarios las activen manualmente en Ayuda > Acerca de Google Chrome.