



Adobe lanzó hoy actualizaciones de software fuera de banda para aplicaciones de After Effects y Media Encoder, que parchean un total de dos nuevas vulnerabilidades críticas.

Ambas vulnerabilidades críticas existen debido a problemas de corrupción de memoria de escritura fuera de los límites y pueden explotarse para ejecutar código arbitrario en sistemas específicos engañando a las víctimas para que abran un archivo especialmente diseñado utilizando el software afectado.

El error [CVE-2020-3765](#) en Adobe After Effects, una aplicación para crear gráficos en movimiento y efectos especiales utilizados en el video, fue descubierto por el investigador de seguridad Matt Powell, e informó a Adobe por medio del proyecto Trend Micro Zero Day Initiative.

El segundo problema, [CVE-2020-3764](#), que afecta a Adobe Media Encoder, un software para codificar y comprimir archivos de audio o video, fue descubierto por el investigador de seguridad canadiense Francis Provencher.

Ninguna de las vulnerabilidades de seguridad corregidas en este lote de actualizaciones de Adobe se divulgó públicamente o se descubrió que se explotaban en la naturaleza, ya que la compañía no encontró evidencia.

Sin embargo, los usuarios de Windows y MacOS siguen siendo altamente recomendados para descargar e instalar las últimas versiones del software afectado para proteger sus sistemas antes de que los hackers comiencen a explotarlos.