Los actores de amenazas han estado aprovechando una vulnerabilidad de día cero previamente desconocida en Adobe Reader mediante documentos PDF manipulados de forma maliciosa desde al menos diciembre de 2025.

El hallazgo, detallado por Haifei Li de EXPMON, ha sido descrito como un exploit de PDF altamente sofisticado. El archivo ("Invoice540.pdf") apareció por primera vez en la plataforma VirusTotal el 28 de noviembre de 2025. Una segunda muestra fue subida a VirusTotal el 23 de marzo de 2026.

Debido al nombre del documento PDF, es probable que exista un componente de ingeniería social, en el que los atacantes engañan a usuarios desprevenidos para que abran los archivos en Adobe Reader. Una vez abierto, se activa automáticamente la ejecución de JavaScript ofuscado con el fin de recopilar información sensible y recibir cargas adicionales.

El investigador de seguridad Gi7w0rm, en una publicación en X, indicó que los documentos PDF analizados contienen señuelos en idioma ruso y hacen referencia a temas vinculados con acontecimientos actuales relacionados con la industria del petróleo y gas en Rusia.

"La muestra funciona como un exploit inicial con la capacidad de recopilar y filtrar diversos tipos de información, potencialmente seguido por exploits de ejecución remota de código (RCE) y de evasión de sandbox (SBX)", señaló Li.

"Hace uso de una vulnerabilidad de día cero/no parcheada en Adobe Reader que le permite ejecutar APIs privilegiadas de Acrobat, y se ha confirmado que funciona en la versión más reciente de Adobe Reader."

Asimismo, cuenta con capacidades para exfiltrar la información recopilada hacia un servidor remoto ("169.40.2[.]68:45191") y recibir código adicional en JavaScript para su ejecución.

Este mecanismo, según explicó Li, podría emplearse para recolectar datos locales, llevar a cabo ataques avanzados de fingerprinting y preparar el terreno para actividades posteriores, incluyendo la entrega de exploits adicionales para lograr la ejecución de código o escapar del

sandbox.

La naturaleza exacta de este exploit de segunda fase sigue siendo desconocida, ya que no se obtuvo respuesta del servidor. Esto podría indicar que el entorno local de pruebas desde el cual se realizó la solicitud no cumplía con los requisitos necesarios para recibir la carga útil.

"Aun así, esta capacidad de día cero/no parcheada para la recolección masiva de información y el potencial de explotación posterior mediante RCE/SBX es suficiente para que la comunidad de seguridad se mantenga en máxima alerta", concluyó Li.