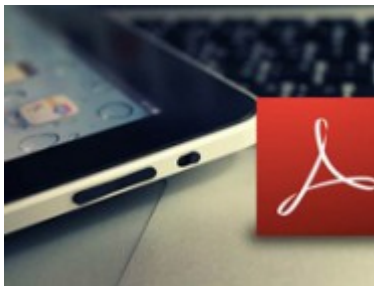


# Descubren una vulnerabilidad Día Cero en el visor de PDF de Adobe

Las últimas jornadas están siendo complicadas para Adobe en materia de seguridad ya que, aparte de [los dos errores](#) que estaban siendo activamente explotados en Flash Player, se ha descubierto una vulnerabilidad Día Cero en su visor de PDF.



Este fallo **permite a los ciberdelincuentes inyectar código malicioso en sistemas de terceros**, según explica [FireEye](#), que ha detectado un documento PDF especialmente diseñado para instalar dos archivos **DLL** en Windows una vez abierto.

Mientras el primero se encarga de cubrir la actividad de su compañero mostrando un mensaje de error falso y abriendo un documento PDF señuelo; el segundo es capaz de conectarse a un dominio remoto a través de HTTP.

Esta mecánica **afecta a las últimas versiones de Adobe Reader, incluyendo 9.5.3, 10.1.5 y 11.0.1**, aunque no se descarta que ediciones anteriores sean también vulnerables.

Esto significa que, para curarse en salud mientras no se lanza ningún parche oficial, **los usuarios deberían evitar usar el programa, deshabilitando el plug-in Adobe PDF en sus navegadores y abriendo sus documentos con otros lectores.**

O, en todo caso, utilizar Acrobat únicamente para abrir documentos procedentes de fuentes de confianza.

Según informa [ArsTechnica](#), el programa de Adobe cuenta con un sistema de “vista protegida” para evitar ataques, pero éste no está activado por defecto. Para habilitarlo hay que ir a Preferencias > Seguridad y revisar las opciones de “Archivos de ubicaciones potencialmente peligrosas” y “Todos los archivos”.