

Embed malicious code into PDF file without security error

Attack on the system through malicious code embedded in PDF files whether users open with the latest version of Adobe Reader or Foxit Reader.

Attack on the system through malicious code embedded in PDF files whether users open with the latest version of Adobe Reader or Foxit Reader.

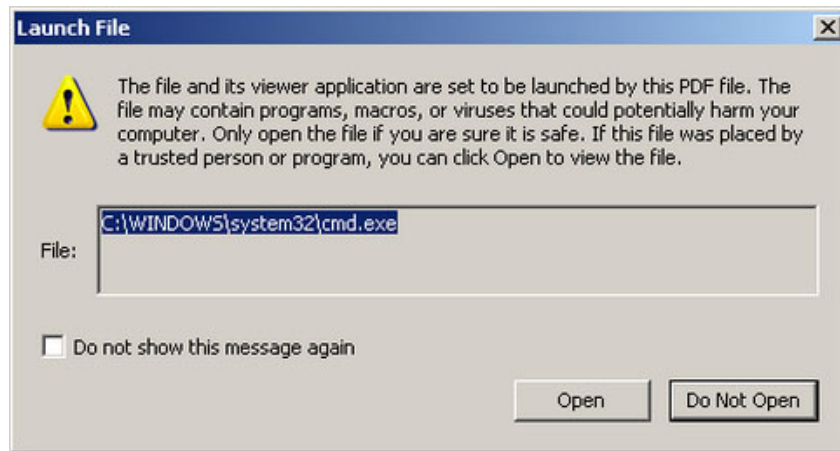


This is shocking information published by security researcher Didier Stevens. The optional code will execute when opening the PDF file with 2 software to view the most popular PDF files currently, Adobe Reader and Foxit Reader without having to exploit any errors from these two software.

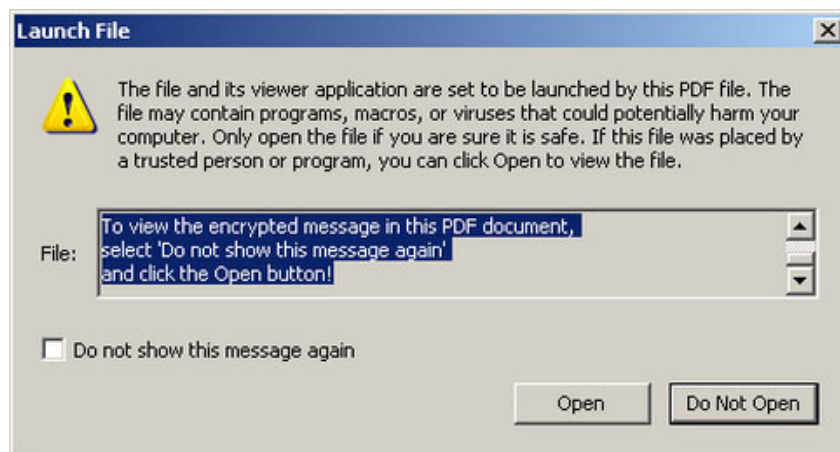
The default setting in the two software for viewing PDF files that do not allow embedding executable code can be run directly, but both are bypassed by a command. This means that users can easily get malicious code when opening PDF files, the type of document file format that is very popular on the internet, using Adobe Reader or Foxit Reader even though both software do not make mistakes. any honey

In the test example demonstrating that it is possible to embed malicious code and execute it easily from within a PDF file, Stevens said he used the option " **Launch Actions / Launch File** " to run the calculator tool that could be replaced by malicious code in a real attack when opening PDF files in Adobe Reader 9.3.1 in Windows XP SP3 and Windows 7 (See the video clip below).

The good news is that Stevens did not announce the exploit code out, but only informed Adobe and Foxit so that these two companies soon find ways to overcome because users are completely passive in case of being attacked by this error. Hackers can completely change the content of Adobe Reader default warning when opening files with embedded executable code.



To open the Windows Command Prompt command window from a PDF file, Adobe Reader forces users to confirm



However, the security message may be changed to mislead users

The idea of this exploit was Jeremy Conway, an independent security researcher " *variation* " new way that hackers can attack. See more information and video clips here.

Adobe's popular products such as Flash Player, PDF or Adobe Reader file formats . have become major targets for hackers because most computers worldwide have applications installed. this. Readers need to be aware of unpublished PDF files or sent from unknown sources, public sharing from the internet and always let the security programs run permanently on the system.

You finished reading the article "**Embed malicious code into PDF file without security error**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.