PDF X-Change Editor

x:xmpmeta

CVE-2018-16303
August 2018

TL;DR

PDF X-Change Editor is a powerful PDF reader able to open and to edit various kinds of documents (PDF, FDF, RTF, pictures ...)

When saving a PDF file, PDF X-Change Editor insert some information about the generation date, the used tool... into an « x:xmpmeta » XML structure. During a PDF document opening, this structure is parsed in order to extract the information which may be retrieved by going to « File > Document Properties > Description ».

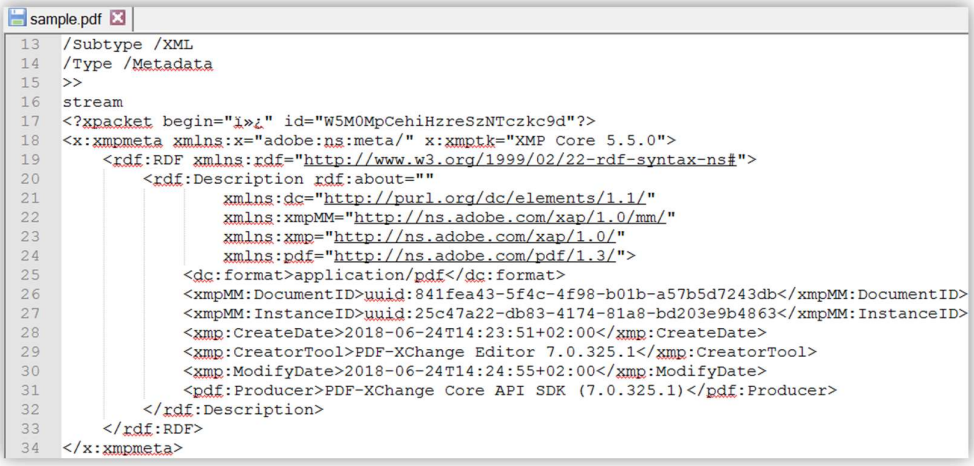

Figure 1 - « x:xmpmeta » structure in a PDF edited by PDF X-Change Editor

Several tests conducted with PDF X-Change Editor 7.0.326.1 allowed to identify an XML external entity injection (XXE) in this structure.

EDIT: Patched since version 7.0.327.0

XML eXternal Entity injection

The XML parser used to process this structure allows the use of XML external entities that can be inserted by tampering the PDF document after generation. The following example contains a small entity used to display « Hello from ENTITY » instead of the « producer » name:

Figure 2 - A « Hello world » XML entity

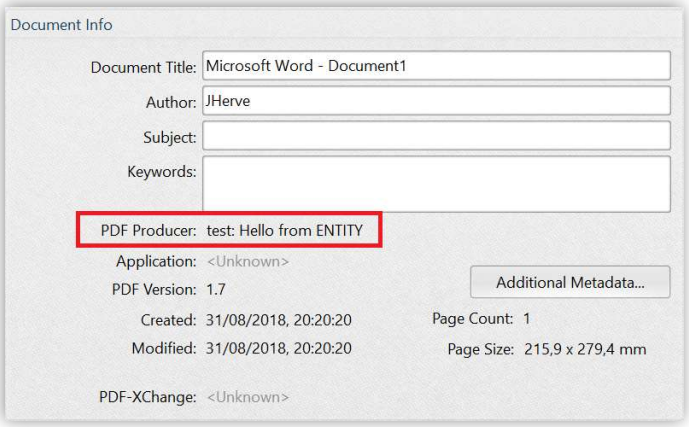

Figure 3 - The entity was successfully inserted in the « producer » field

Such external entity may be used in a « recursive » way (known as « Billion laughs attack »: https://en.wikipedia.org/wiki/Billion_laughs_attack) to create malicious PDF documents that would consume a large amount of memory during parsing and result in a denial of service:

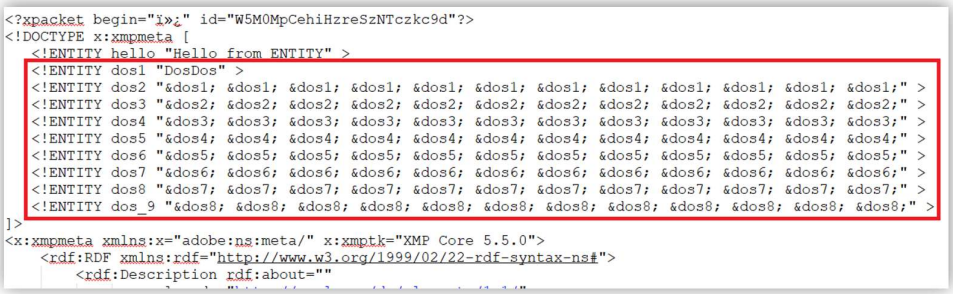

Figure 4 - A billion laughs attack

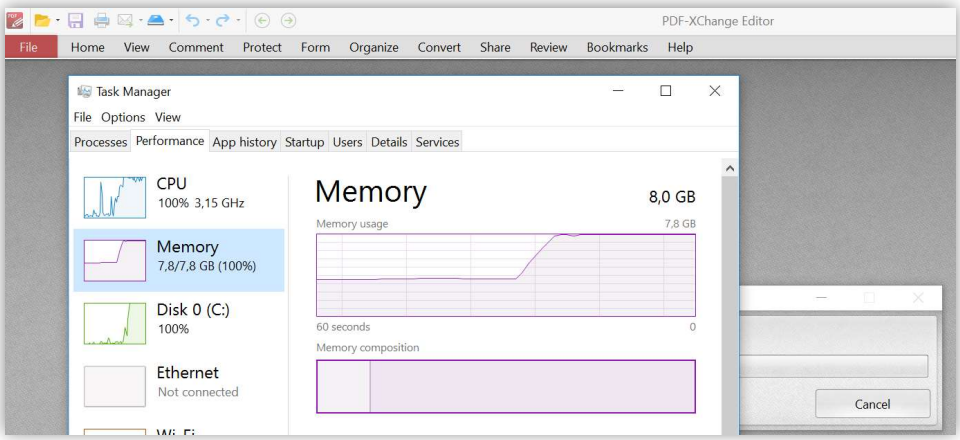

Figure 5 - Trying to open the PDF leads to a denial of service

In some cases, this kind vulnerability may also be used to read or download files and, in worst case leads to command execution on the affected system as shown on this document: https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing. However, such scenarios do not seem to be possible with PDF X-Change Editor.

Moreover, when installed on Windows, PDF-XChange Editor seems to be used by the windows explorer to load and display the producer name when the cursor is on the PDF file icon. In such case, the denial of service may happen even if the user does not try to open the file.

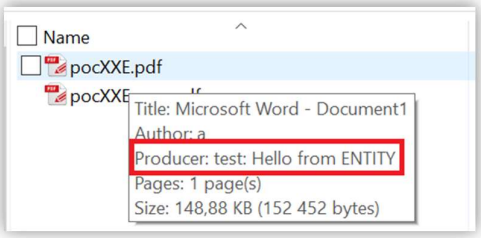

Figure 6 - The « producer » name is displayed by the windows explorer