

This document details the information security vulnerability inherent in the PowerPDF Advanced as tested in the latest version seen here:

Nuance Power PDF Advanced  
Powered by Zeon DocuCom and OmniPage OCR.

Product Information  
Version: 1.1

Copyright © 1995-2015 Nuance Communications, Inc. All rights reserved.

## Vulnerability

The software permits the encoding/editing of “meta data” such as Title, Author, Subject, Keywords, etc... When the information is removed or overwritten within the interface, it appears that the previous information is lost. However, the information remains within the PDF file. This is a leak of potentially sensitive information after a user believes they have edited or removed it.

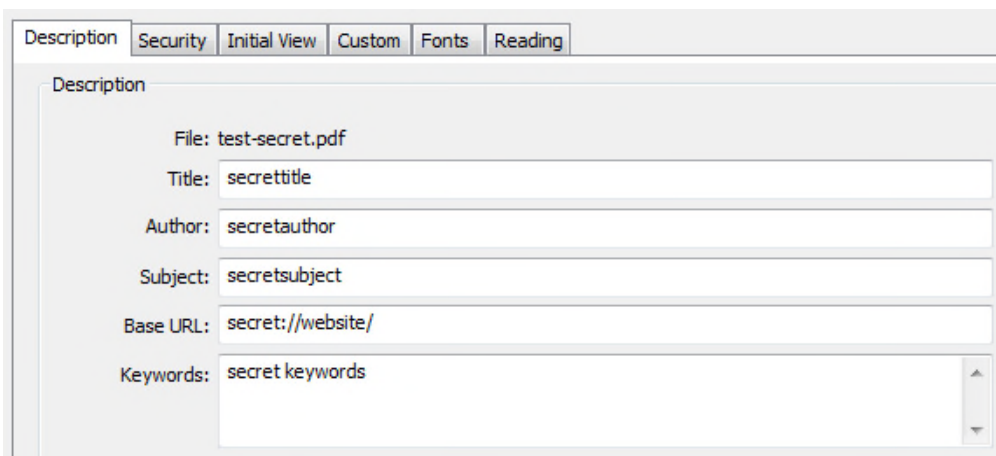
## Impact

Individuals or organizations wishing to protect sensitive meta-data of a PDF file may be unable to do so. This may cause the inadvertent leakage of information (previous authors, keywords, subjects,titles, etc..) that an individual or organization does not wish to expose.

## Reproducibility

The following steps reproduce and demonstrate the problem:

1. Open or create a PDF document and write meta-data into the document. For example, the following:



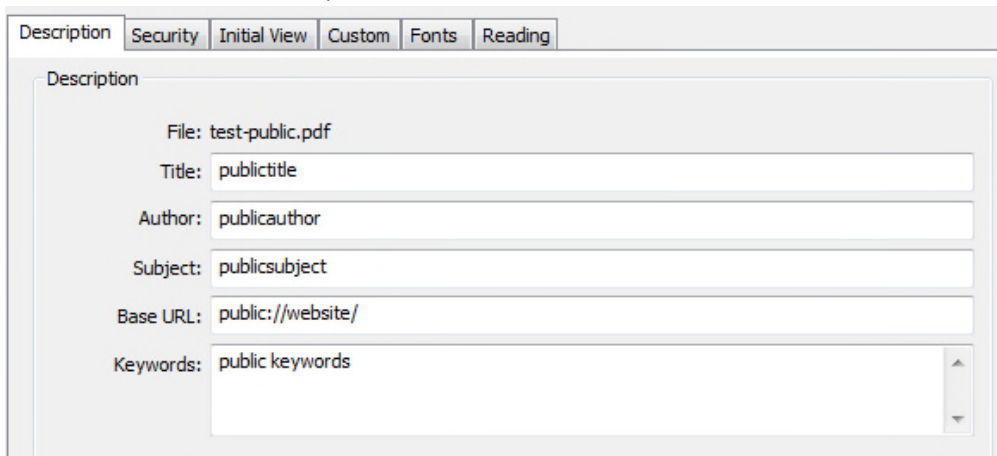
The screenshot shows the 'Description' tab of the PowerPDF Advanced interface. The 'File' is 'test-secret.pdf'. The 'Title' field contains 'secrettitle', 'Author' contains 'secretauthor', 'Subject' contains 'secretsubject', 'Base URL' contains 'secret://website/', and 'Keywords' contains 'secret keywords'. The interface has a tabbed structure with 'Description', 'Security', 'Initial View', 'Custom', 'Fonts', and 'Reading' tabs.

2. Save the document. You can use “pdftinfo” or “strings” to view the meta data:

```
C:\temp> pdftinfo test-secret.pdf
Title:          secrettitle
Subject:        secretsubject
Keywords:       secret keywords
Author:         secretauthor
Creator:        test-secret - Notepad
Producer:       Nuance PDF Create
CreationDate:   07/07/15 13:21:40
ModDate:        07/07/15 13:22:56
Tagged:         no
Form:           none
Pages:          1
Encrypted:      no
Page size:      612 x 792 pts (letter) (rotated 0 degrees)
File size:      19394 bytes
Optimized:      yes
PDF version:    1.5
```

```
C:\temp> strings test-secret.pdf | grep "secret"
<xap:CreatorTool>test-secret - Notepad</xap:CreatorTool>
<rdf:li xml:lang="x-default">test-secret - Notepad</rdf:li>
<pdf:Keywords>secret keywords</pdf:Keywords>
<xap:CreatorTool>test-secret - Notepad</xap:CreatorTool>
<rdf:li xml:lang="x-default">secrettitle</rdf:li>
<rdf:li>secretauthor</rdf:li>
<rdf:li xml:lang="x-default">secretsubject</rdf:li>
<</Creator(test-secret - Notepad)/Producer(Nuance PDF
Create)/CreationDate(D:201
50707132140-04'00')/ModDate(D:20150707132256-
04'00')/Author(secretauthor)/Title(
secrettitle)/Subject(secretsubject)/Keywords(secret keywords)>>
<</Type/Catalog/Pages 4 0 R/PageMode/UseNone/Metadata 1 0
R/URI<</Base(secret://
website/)>>>>
```

3. Close PowerPDF Advanced and reopen. This time, edit the values to something else, as demonstrated in this example:



4. Now examine the file with the 'pdftinfo' utility again. It appears to properly show the "public" information in this example, indicating that the meta data has been overwritten:

```
C:\temp> pdftinfo test-public.pdf
Title:          publictitle
Subject:        publicsubject
Keywords:       public keywords
Author:         publicauthor
Creator:        test-secret - Notepad
Producer:       Nuance PDF Create
CreationDate:   07/07/15 13:21:40
ModDate:        07/07/15 13:23:49
Tagged:         no
Form:           none
Pages:          1
Encrypted:      no
Page size:      612 x 792 pts (letter) (rotated 0 degrees)
File size:      21166 bytes
Optimized:      yes
PDF version:    1.5
```

5. **However**, when viewing the file contents with 'strings', the PDF file is shown to have retained a copy of the original meta data:

```
C:\temp> strings test-public.pdf | grep "secret"
<xap:CreatorTool>test-secret - Notepad</xap:CreatorTool>
<rdf:li xml:lang="x-default">test-secret - Notepad</rdf:li>
<pdf:Keywords>secret keywords</pdf:Keywords>
<xap:CreatorTool>test-secret - Notepad</xap:CreatorTool>
<rdf:li xml:lang="x-default">secrettitle</rdf:li>
<rdf:li>secretauthor</rdf:li>
<rdf:li xml:lang="x-default">secretsubject</rdf:li>
<</Creator(test-secret - Notepad)/Producer(Nuance PDF
Create)/CreationDate(D:201
50707132140-04'00')/ModDate(D:20150707132256-
04'00')/Author(secretauthor)/Title(
secrettitle)/Subject(secretsubject)/Keywords(secret keywords)>>
<</Type/Catalog/Pages 4 0 R/PageMode/UseNone/Metadata 1 0
R/URI<</Base(secret://
website/)>>>>
<xap:CreatorTool>test-secret - Notepad</xap:CreatorTool>
<</Creator(test-secret - Notepad)/Producer(Nuance PDF
Create)/CreationDate(D:201
50707132140-04'00')/ModDate(D:20150707132349-
04'00')/Author(publicauthor)/Title(
publictitle)/Subject(publicsubject)/Keywords(public keywords)>>
```