

Forum:[Hack Forums](#)

Thread: [PDF EXPLOIT /LNK/REG/DOC/](#)

dmoreki81 - December 6, 2024, 3:42 am

Hello Guys,

I have written different programs that can be used as exploit to gain access, but I got to understand that some of the exploits like PDF, acts as a carrier while others can't upload via email server.

Now here is my simple question, which can be embedded into a PDF Dropper that will not trigger when downloaded via Chrome or Edge. Because during downloading, Chrome always sends a warning message, likewise Edge.

Secondly, Files like Reg, when downloaded shows a UAC warning when run. (Warning! Do you trust this program). Is there a way this can be Bypassed?

Thirdly, I have noticed that DOC files can no longer work as exploit as VBA is being flagged by most antivirus and Windows defender.

Fourthly, Is there a better way that PDF can act directly when run to execute a program at the background using either CMD or Powershell that will work on browsers as well as most people are moving away from reader apps and using browsers to view pdf files. If it's not possible, which will you suggest as the best method for PDF exploit via browser.

I am here to learn and open to new ideas. Your suggestions and advise will go a long way in reshaping my thinking method and enhancing my coding skills

Thanks

DramaKing - December 6, 2024, 4:36 am

(Dec 6, 2024 04:42 AM)dmoreki81 Wrote: [\[CITE\]](#) Hello Guys,

I have written different programs that can be used as exploit to gain access, but I got to understand that some of the exploits like PDF, acts as a carrier while others can't upload via email server.

Now here is my simple question, which can be embedded into a PDF Dropper that will not trigger when downloaded via Chrome or Edge. Because during downloading, Chrome always sends a warning message, likewise Edge.

Secondly, Files like Reg, when downloaded shows a UAC warning when run. (Warning! Do you trust this program). Is there a way this can be Bypassed?

Thirdly, I have noticed that DOC files can no longer work as exploit as VBA is being flagged by most antivirus and Windows defender.

Fourthly, Is there a better way that PDF can act directly when run to execute a program at the background using either CMD or Powershell that will work on browsers as well as most people are moving away from reader apps and using browsers to view pdf files. If it's not possible, which will you suggest as the best method for PDF exploit via browser.

I am here to learn and open to new ideas. Your suggestions and advise will go a long way in reshaping my thinking method and enhancing my coding skills

Thanks

There are multiple ways that Safe Browsing and SmartScreen will trigger warnings and block downloads. See here:

<https://hackforums.net/showthread.php?tid=6244776&highlight=safe+browsing>

That doesn't sound like UAC. It's probably due to MotW.

Forget antivirus. Office macros have been disabled for years.

No, of course PDFs can't run system commands or executables outside a browser sandbox. Not for a long time, certainly. If there was a sandbox escape exploit that could do this, it would be patched within weeks of being discovered and pushed to every running browser within a few days.

Binance - December 7, 2024, 3:38 pm

(Dec 6, 2024 05:06 AM)Yung Zel Wrote: [\[CITE\]](#) If you're talking about a malicious file warning that's because the server it's being downloaded from isn't recognized by the browser as a trusted source so it'll need to be aged.

Yes by registry hijacking but I'm not sure on the current effectiveness. A signing certificate is the way most parties go but there's a lot of scammers attempting to sell these and you'd have to find a trusted seller to provide one.

This isn't a question, what are you asking?

SE is the most commonly used technique at the moment as far as I'm aware.

Holy fuck look at you go.

If I could give you a diploma I would.

titan2xx - December 9, 2024, 3:10 pm

Is there any good PDF Exploit out there? Who knows where I can get one?

Ph4n70M Phr34K - December 9, 2024, 3:19 pm

(Dec 9, 2024 04:10 PM)titan2xx Wrote: [\[CITE\]](#) Is there any good PDF Exploit out there? Who knows where I can get one?

You cant get one. Such exploits doesn't exist in today's technological landscape.

Joskyte - December 10, 2024, 8:52 am

You can put your file in a rar make it look like a pdf ending. I think that should work. How do you get your rat fully UD is my question?

titan2xx - December 10, 2024, 11:24 am

(Dec 9, 2024 04:19 PM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) You cant get one. Such exploits doesn't exist in today's technological landscape.

How do you that?

777extremegamer - December 12, 2024, 6:01 pm

This is awesome wow ?

csslll - February 1, 2025, 6:51 am

can you provide link to this software?

Hackers - February 1, 2025, 12:18 pm

(Dec 6, 2024 05:06 AM)Yung Zel Wrote: [\[CITE\]](#) SE is the most commonly used technique at the moment as far as I'm aware.

This is what I think too. There may be some methods around, but I feel like the biggest flaw in cybersecurity is the people using devices. Not the software or hardware.

albert-berti - February 1, 2025, 2:16 pm

Really working 100% ?

dmoreki81 - February 25, 2025, 2:55 am

Can an Office application run on Silent? I have been looking for a way around this for years without having any success. What is the best method that can be used as a carrier for a payload

bluff_bluff - February 26, 2025, 3:08 am

(Dec 6, 2024 04:42 AM)dmoreki81 Wrote: [\[CITE\]](#) Hello Guys,

I have written different programs that can be used as exploit to gain access, but I got to understand that some of the exploits like PDF, acts as a carrier while others can't upload via email server.

Now here is my simple question, which can be embedded into a PDF Dropper that will not trigger when downloaded via Chrome or Edge. Because during downloading, Chrome always sends a warning message, likewise Edge.

Secondly, Files like Reg, when downloaded shows a UAC warning when run. (Warning! Do you trust this program). Is there a way this can be Bypassed?

Thirdly, I have noticed that DOC files can no longer work as exploit as VBA is being flagged by most antivirus and Windows defender.

Fourthly, Is there a better way that PDF can act directly when run to execute a program at the background using either CMD or Powershell that will work on browsers as well as most people are moving away from reader apps and using browsers to view pdf files. If it's not possible, which will you suggest as the best method for PDF exploit via browser.

I am here to learn and open to new ideas. Your suggestions and advise will go a long way in reshaping my thinking method and enhancing my coding skills

Thanks

As others have mentioned, PDF exploits are very difficult nowadays. However, if you are not restricted to Chrome and Edge, there might be an option. A relatively recent vulnerability from May of 2024, CVE-2024-4367, has been found in PDF.js. That means that Firefox, Foxit, and I believe Thunderbird email client (?) are directly vulnerable to a javascript injection. You can even get the injection to call-back to you and grab code that can lead to remote code execution, which means you can keep the embedded injection quite small and just call-back to grab a separate exploit (getting around AV with this type of thing is quite tricky however).

There is a PoC for Firefox and Foxit on github: search for "rzte pdf-exploit github" and it will appear right away. As you can see the author manages to pop calc.exe on Foxit and an alert on Firefox. The first exploit requires user input, but the second runs immediately. Getting a user to disable a warning can be tricky nowadays as most people pay attention to pop-up warnings, but you could get

lucky. The pop-up alert could be more dangerous if you can get it to run in the background (like with a call-back).

This PDF.js vulnerability is perhaps a bit more dangerous than it seems as it can be readily invoked in the background by certain programs (if I understand things correctly). Check out the Youtube video by Snyk researchers by searching for: "Afraid of PDF files PDF.js Snyk"

You can also search for "CryptoCat XSS in PDF.js" on Youtube and you will get a really informative video on how to abuse PDF.js (in a very simple manner that isn't particularly realistic in real-world applications, but it provides excellent background information and some simple tricks for modifying test payloads).

Good luck

You would have to do a ton of work to get this working, but if you are attempting to get things onto a system that isn't updated consistently, you might be able to get it working.

dmoreki81 - February 28, 2025, 11:41 pm

(Feb 26, 2025 04:08 AM)bluff_bluff Wrote: [\[CITE\]](#) As others have mentioned, PDF exploits are very difficult nowadays. However, if you are not restricted to Chrome and Edge, there might be an option. A relatively recent vulnerability from May of 2024, CVE-2024-4367, has been found in PDF.js. That means that Firefox, Foxit, and I believe Thunderbird email client (?) are directly vulnerable to a javascript injection. You can even get the injection to call-back to you and grab code that can lead to remote code execution, which means you can keep the embedded injection quite small and just call-back to grab a separate exploit (getting around AV with this type of thing is quite tricky however).

There is a PoC for Firefox and Foxit on github: search for "rzte pdf-exploit github" and it will appear right away. As you can see the author manages to pop calc.exe on Foxit and an alert on Firefox. The first exploit requires user input, but the second runs immediately. Getting a user to disable a warning can be tricky nowadays as most people pay attention to pop-up warnings, but you could get lucky. The pop-up alert could be more dangerous if you can get it to run in the background (like with a call-back).

This PDF.js vulnerability is perhaps a bit more dangerous than it seems as it can be readily invoked in the background by certain programs (if I understand things correctly). Check out the Youtube video by Snyk researchers by searching for: "Afraid of PDF files PDF.js Snyk"

You can also search for "CryptoCat XSS in PDF.js" on Youtube and you will get a really informative video on how to abuse PDF.js (in a very simple manner that isn't particularly realistic in real-world applications, but it provides excellent background information and some simple tricks for modifying test payloads).

Good luck

You would have to do a ton of work to get this working, but if you are attempting to get things onto a system that isn't updated consistently, you might be able to get it working.

This is quite informative. Thank you. Do you know of any Exploit that is very potent and can have a success rate of 80-90% and can attach via email.

coconot432 - March 5, 2025, 9:29 am

wow so much great informatation on a single post

