

Forum:[Hack Forums](#)

Thread: [\[Fallen\] Actual PDF exploit that works](#)

DramaKing - May 24, 2024, 12:41 pm

And it doesn't even require a 12-year-old version of Adobe Reader. The exploit downloads and executes malicious payloads when the infected PDF file is opened with current versions of Foxit PDF Reader (<2024.3) and users accept the warning messages. Read the details [here](#). No PoC is available.

jasrrow - May 29, 2024, 6:29 am

when PDF is opened, it is exploiting system or how does that work ?

DramaKing - May 29, 2024, 8:21 am

It exploits the PDF reader. There's literally an illustration of the exploit chain at the top of that article.

Scrubspooft - May 29, 2024, 6:59 pm

Why would anyone not use a standard browser to open/edit/print PDFs in 2024?

Burger - May 29, 2024, 7:45 pm

I had to show this to my Security Team at my work because we use Foxit PDF on almost every system deployed for employees. We only open PDFs mainly with our business however some folks use it for metrics and share between other companies and such so I made sure they were aware of this CVE.

Long story short my security team loves me because I bring new CVEs to them weekly that could affect us as a whole. I would like to think I'm very secure person and have good security measures put in place either physically or within my own brain. But if someone in my company got infected then it could affect me so I take it very seriously.

Scrubspooft - May 29, 2024, 7:53 pm

(May 29, 2024 07:45 PM)Burger Wrote: [\[CITE\]](#) I had to show this to my Security Team at my work because we use Foxit PDF on almost every system deployed for employees. We only open PDFs mainly with our business however some folks use it for metrics and share between other companies and such so I made sure they were aware of this CVE.

Long story short my security team loves me because I bring new CVEs to them weekly that could affect us as a whole. I would like to think I'm very secure person and have good security measures put in place either physically or within my own brain. But if someone in my company got infected then it could affect me so I take it very seriously.

As security, why use external software to open PDFs in 2024?

Burger - May 30, 2024, 5:52 am

(May 29, 2024 07:53 PM)Scrubspooft Wrote: [\[CITE\]](#) As security, why use external software to open PDFs in 2024?

I do not control the stack of what we use at my Company. I am not in the control group for any of that, I have my own specialized team I lead however we follow what the man above says to do and use.

Honestly yes we can use Chrome or whatever as a PDF Viewer however we do a lot of signing and such with Forms for ISP, Client contracts, etc.

Brill - May 31, 2024, 12:06 am

(May 29, 2024 08:21 AM)DramaKing Wrote: [\[CITE\]](#) It exploits the PDF reader. There's literally an illustration of the exploit chain at the top of that article.

isn't fallen supposed to be a 1337 hacker group. go ahead and explain to him how it works considering your post is nothing more than a glorified headline. no need to get passive aggressive due to a response in your brainrot thread

'a pdf exploit that works' there's many methods that work on a plethora of readers. this is not new nor uncommon. hence the long list of cves published in 2024 targeting foxit alone

https://www.cvedetails.com/vulnerability-list/vendor_id-6467/product_id-10925/Foxit-Pdf-Reader.html
!

takes 2 seconds to find technical details regarding this exploit (assuming you have any knowledge about what you create these glorified headlines about, which in your defence is rare on hf these days)

happygonutty - May 31, 2024, 5:36 pm

(May 29, 2024 11:20 PM)Yung Zel Wrote: [\[CITE\]](#) Aren't you just a good little soldier helping out your boss!

Yeah burger, I agree with Yung Zel. In my work or people I work with, I never share CVEs to them since I believe it wouldn't affect my paycheck or salary. I guess you just happen to be the typical good white hat who wants to keep things at bay. ?

DramaKing - May 31, 2024, 5:51 pm

(May 31, 2024 05:36 PM)happygonutty Wrote: [\[CITE\]](#) Yeah burger, I agree with Yung Zel. In my work or people I work with, I never share CVEs to them since I believe it wouldn't affect my paycheck or salary. I guess you just happen to be the typical good white hat who wants to keep things at bay. ?

Your company getting hit with a cyber attack is never good. Even if nothing happens, you could make a good impression as to your value as a worker.

happygonutty - May 31, 2024, 6:02 pm

(May 31, 2024 05:51 PM)DramaKing Wrote: [\[CITE\]](#) Your company getting hit with a cyber attack is never good. Even if nothing happens, you could make a good impression as to your value as a worker.

Well you are right but sometimes its best that you also benefit from it if it is not your role in the company or you are asked to do it. But if cyber attacks are your responsibilities (I believe OP is responsible for this) then sure why not, I would definitely report new CVEs weekly as well regardless if it goes to paycheck or not.

thisisfoz - June 5, 2024, 6:49 pm

This has been in the wild for about a year, if not longer. It's no longer fud and has too many clicks. It's trash.

powisi3138 - September 29, 2024, 1:51 pm

i'm definitely following this thread. nice

choucha3dz - October 2, 2024, 1:05 am

found this video myb still working [deleted] how test it ?

DramaKing - October 2, 2024, 4:45 am

(Oct 2, 2024 01:05 AM)choucha3dz Wrote: [\[CITE\]](#) found this video myb still working
youtu.be/o9UllS3Sxjk how test it ?

Hack-Tools.net is a scam.

I think that @Snyke@ put it well on something similar. [RE: inquiry](#)

Biggy_Asian - October 6, 2024, 1:43 pm

(May 29, 2024 08:21 AM)DramaKing Wrote: [\[CITE\]](#) It exploits the PDF reader. There's literally an illustration of the exploit chain at the top of that article.

Interesting so I am guessing its some sort of RCE/XSS with reading the PDF file? I have never really heard of Foxit so I cannot say for sure... Looks cool though nice find.

DramaKing - October 6, 2024, 3:17 pm

(Oct 6, 2024 01:43 PM)Biggy_Asian Wrote: [\[CITE\]](#) Interesting so I am guessing its some sort of RCE/XSS with reading the PDF file? I have never really heard of Foxit so I cannot say for sure... Looks cool though nice find.

The article explains it, but yes, malicious commands get executed when the file is opened.