RQ4: Fuzzing Campaign

This experiment is in the `Section V-E Vulnerability Discovery` of our paper. The goal of this experiment is to measure the accuracy of the type information infered by TYPEORACLE. The result is shown in the `TABLE II: Discovered Zero-Day Vulnerabilities` in our paper. To evaluate the vulnerability discovery capabilities of different fuzzers in the wild, we deploy 2-week fuzzing campaign for each fuzzer. Gramatron+, Favocado, Cooper, TYPEORACLE, Favocado+TYPEORACLE and Cooper+TYPEORACLE report 2, 6, 5, 33, 10, 18 unique crashes respectively. Further inspection on the crash reports result in 38 zero-day vulnerabilities, as detailed in Table II. Even within the first 48 hours, TYPEORACLE exposed 18 vulnerabilities, which is 2.57 times that of the best of other fuzzers.

folder structure

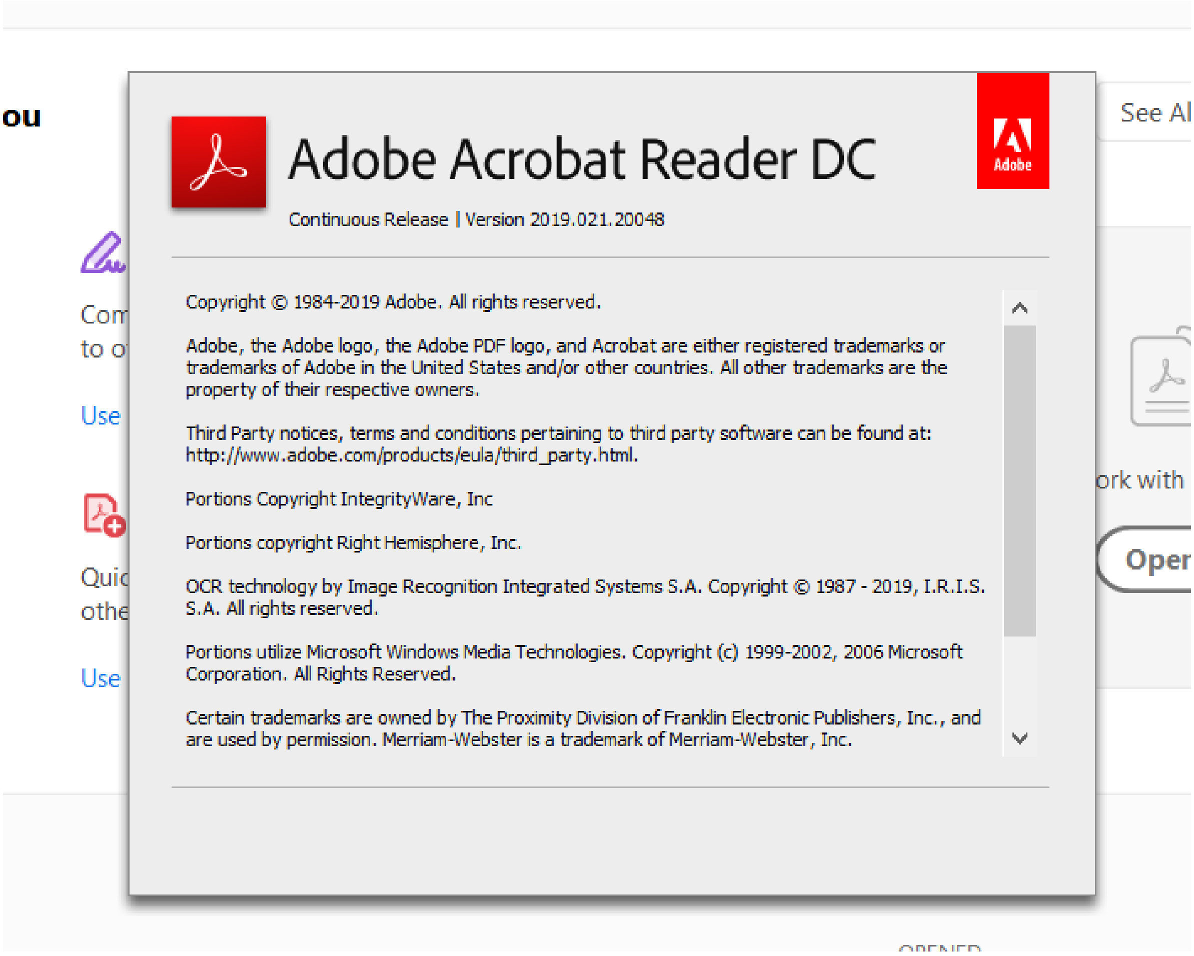
```
- adobe reader (this folder contains all the vulnerabilities TypeOracle have
found on Adobe Reader)

- foxit reader (this folder contains all the vulnerabilities TypeOracle have
found on Foxit Reader)
```

how to reproduce

Adobe Reader

1. make sure you have the correct version of Adobe Reader and change the default PDF Reader to Adobe Reader(please refer to Other/Installers/README.pdf for the installation)， also add the folder to Priviledge Location(please refer to Other/Tips.pdf for how to add to Priviledge Location).



Adobe Acrobat Reader DC

Continuous Release | Version 2019.021.20048

Copyright © 1984-2019 Adobe. All rights reserved.

Adobe, the Adobe logo, the Adobe PDF logo, and Acrobat are either registered trademarks or trademarks of Adobe in the United States and/or other countries. All other trademarks are the property of their respective owners.

Third Party notices, terms and conditions pertaining to third party software can be found at: http://www.adobe.com/products/eula/third_party.html.

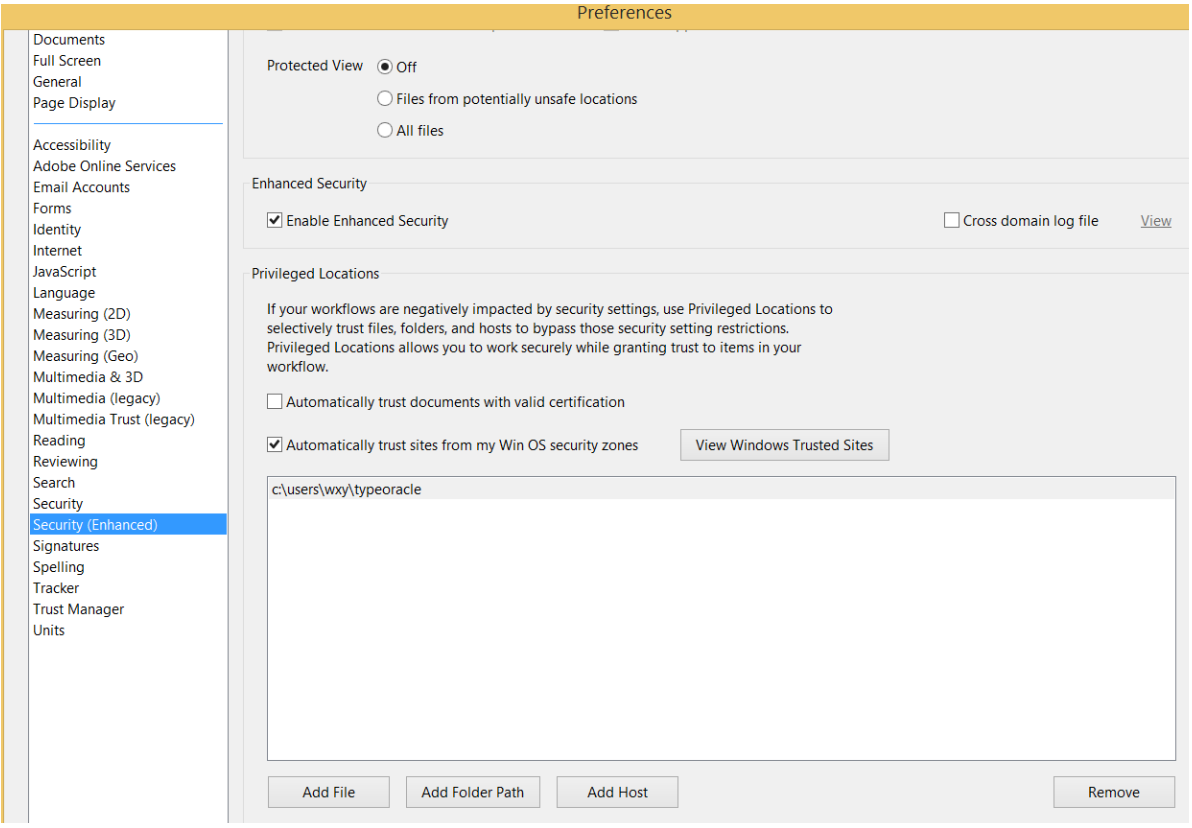
Portions Copyright IntegrityWare, Inc

Portions copyright Right Hemisphere, Inc.

OCR technology by Image Recognition Integrated Systems S.A. Copyright © 1987 - 2019, I.R.I.S. S.A. All rights reserved.

Portions utilize Microsoft Windows Media Technologies. Copyright (c) 1999-2002, 2006 Microsoft Corporation. All Rights Reserved.

Certain trademarks are owned by The Proximity Division of Franklin Electronic Publishers, Inc., and are used by permission. Merriam-Webster is a trademark of Merriam-Webster, Inc.



Preferences

Protected View ● Off

○ Files from potentially unsafe locations

○ All files

Enhanced Security

☑ Enable Enhanced Security □ Cross domain log file View

Privileged Locations

If your workflows are negatively impacted by security settings, use Privileged Locations to selectively trust files, folders, and hosts to bypass those security setting restrictions. Privileged Locations allows you to work securely while granting trust to items in your workflow.

□ Automatically trust documents with valid certification

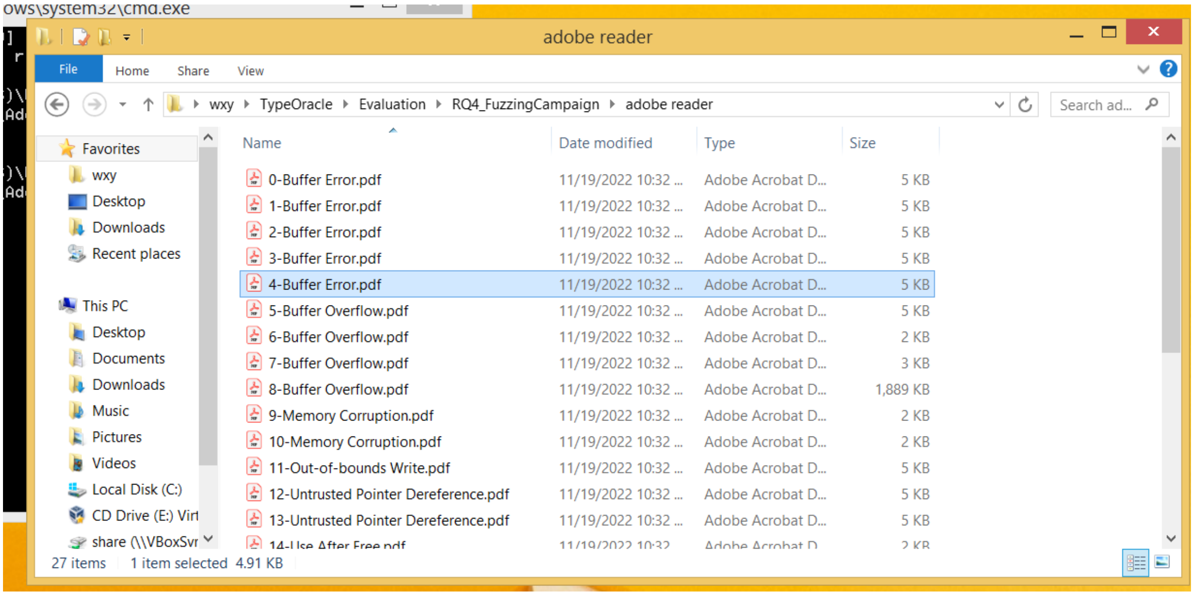
☑ Automatically trust sites from my Win OS security zones View Windows Trusted Sites

c:\users\wxy\typeoracle

2. turn on the Page Heap

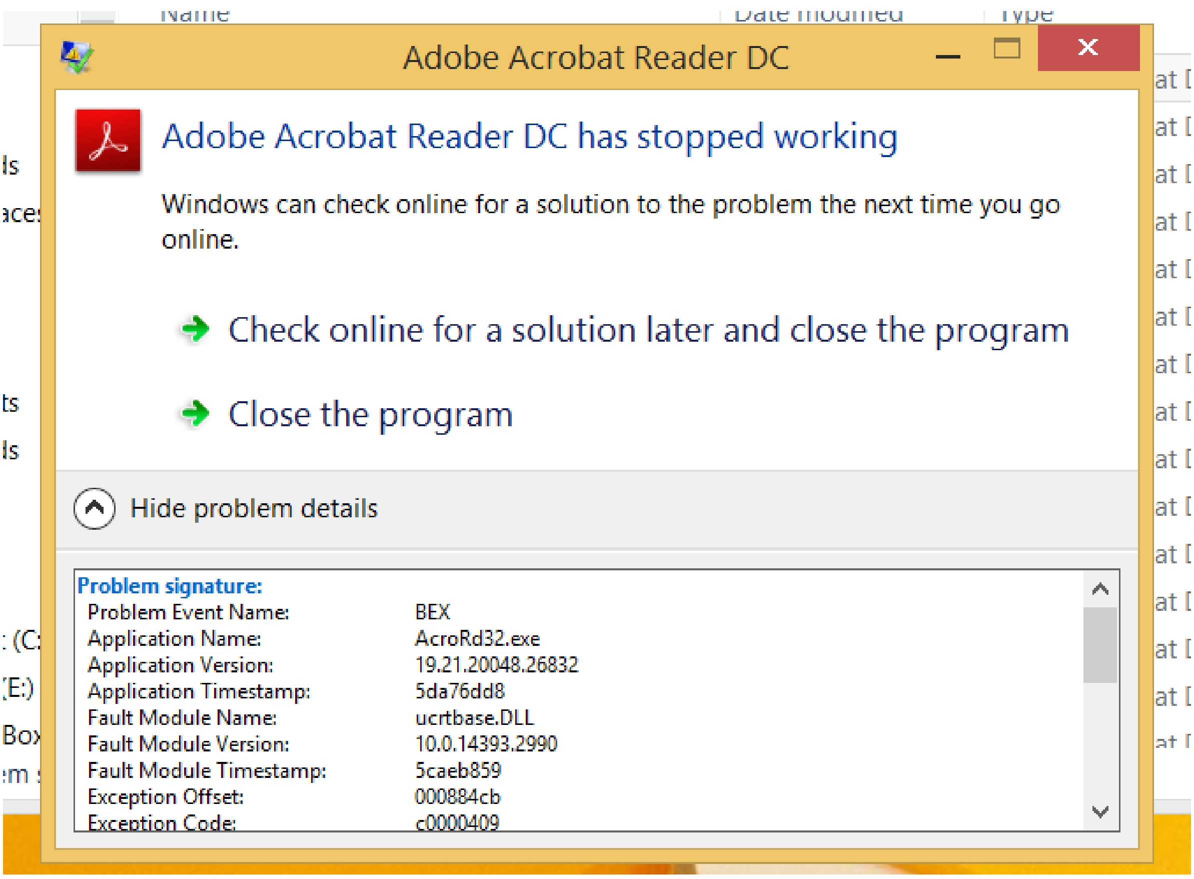
```
"C:\Program Files (x86)\Windows Kits\8.1\Debuggers\x86\gflags.exe" /p /enable
"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe"
```

3. open any of them and Adobe Reader will crash



Name	Date modified	Type	Size
0-Buffer Error.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	5 KB
1-Buffer Error.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	5 KB
2-Buffer Error.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	5 KB
3-Buffer Error.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	5 KB
4-Buffer Error.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	5 KB
5-Buffer Overflow.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	5 KB
6-Buffer Overflow.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	2 KB
7-Buffer Overflow.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	3 KB
8-Buffer Overflow.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	1,889 KB
9-Memory Corruption.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	2 KB
10-Memory Corruption.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	2 KB
11-Out-of-bounds Write.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	5 KB
12-Untrusted Pointer Dereference.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	5 KB
13-Untrusted Pointer Dereference.pdf	11/19/2022 10:32 ...	Adobe Acrobat D...	5 KB
14-Use After Free.pdf	11/19/2022 10:32	Adobe Acrobat D	2 KB

27 items 1 item selected 4.91 KB



Adobe Acrobat Reader DC

Adobe Acrobat Reader DC has stopped working

Windows can check online for a solution to the problem the next time you go online.

→ Check online for a solution later and close the program

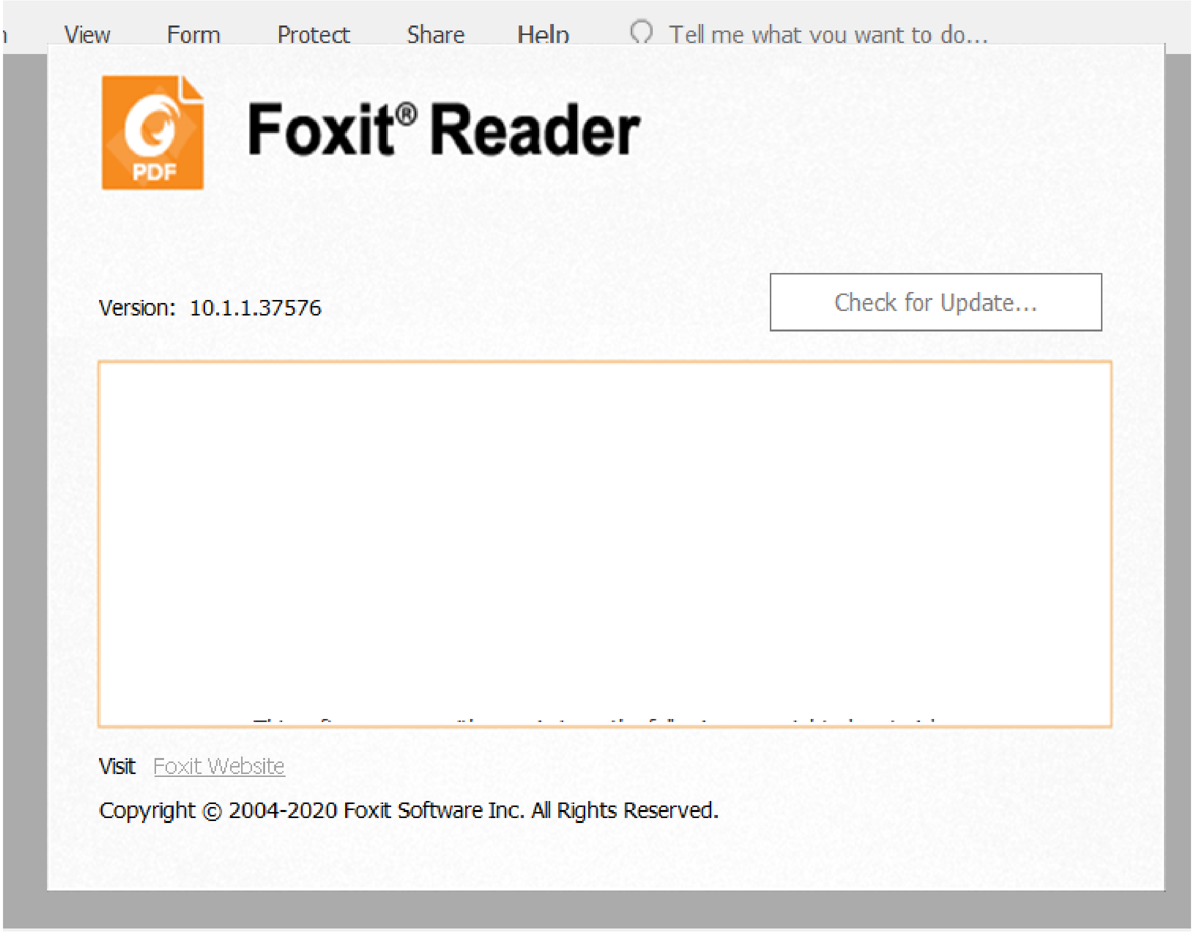
→ Close the program

Hide problem details

```
Problem signature:
  Problem Event Name:            BEX
  Application Name:              AcroRd32.exe
  Application Version:           19.21.20048.26832
  Application Timestamp:         5da76dd8
  Fault Module Name:             ucrtbase.DLL
  Fault Module Version:          10.0.14393.2990
  Fault Module Timestamp:        5caeb859
  Exception Offset:              000884cb
  Exception Code:                c0000409
```

Foxit Reader

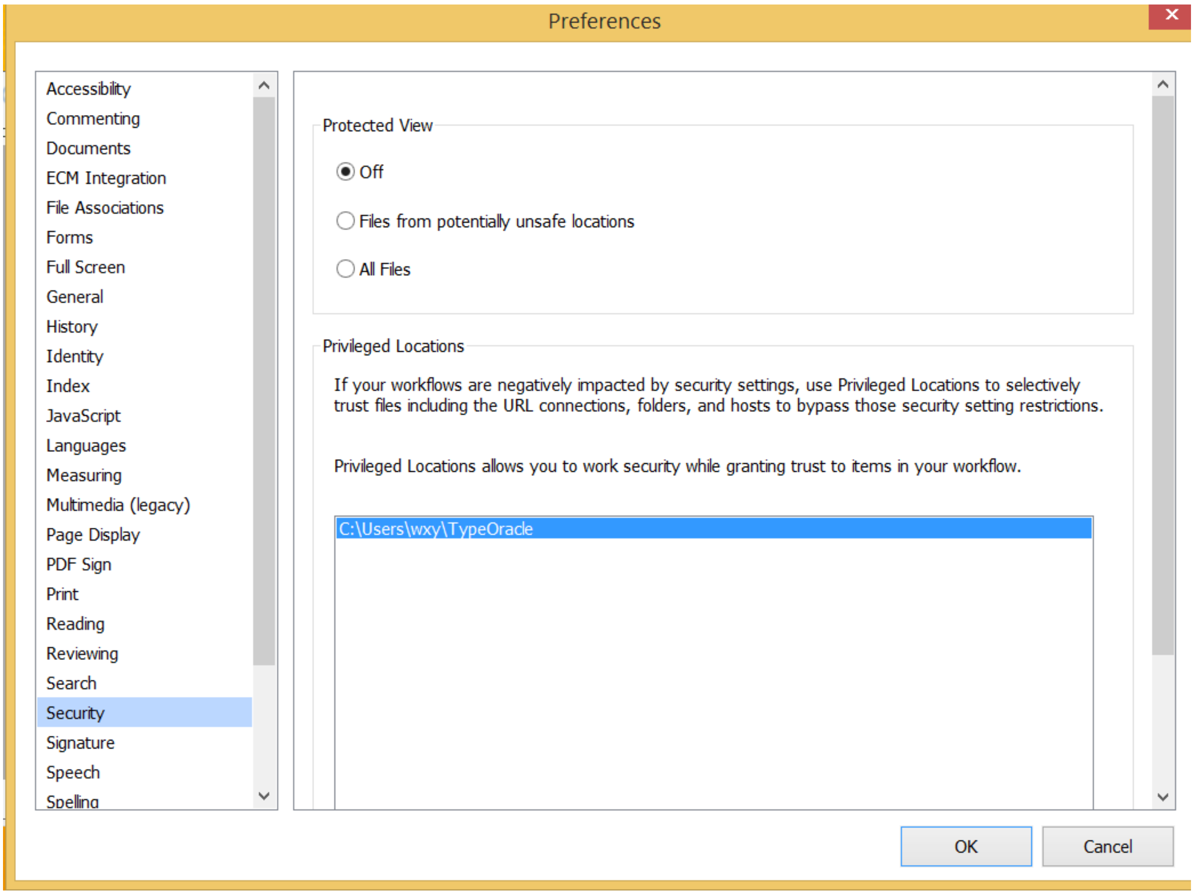
1. make sure you have the correct version of Foxit Reader and change the default PDF Reader to Foxit Reader(please refer to Other/Installers/README.pdf for the installation), also add the folder to Priviledge Location(please refer to Other/Tips.pdf for how to add to Priviledge Location).



Version: 10.1.1.37576

Visit Foxit Website

Copyright © 2004-2020 Foxit Software Inc. All Rights Reserved.



Protected View

● Off

○ Files from potentially unsafe locations

○ All Files

Privileged Locations

If your workflows are negatively impacted by security settings, use Privileged Locations to selectively trust files including the URL connections, folders, and hosts to bypass those security setting restrictions.

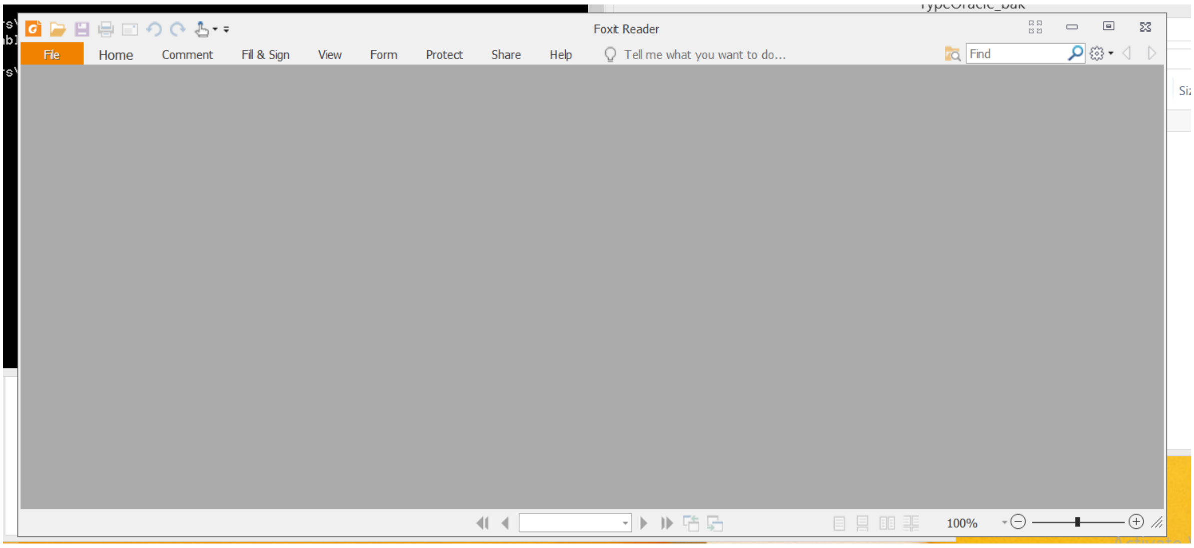
Privileged Locations allows you to work security while granting trust to items in your workflow.

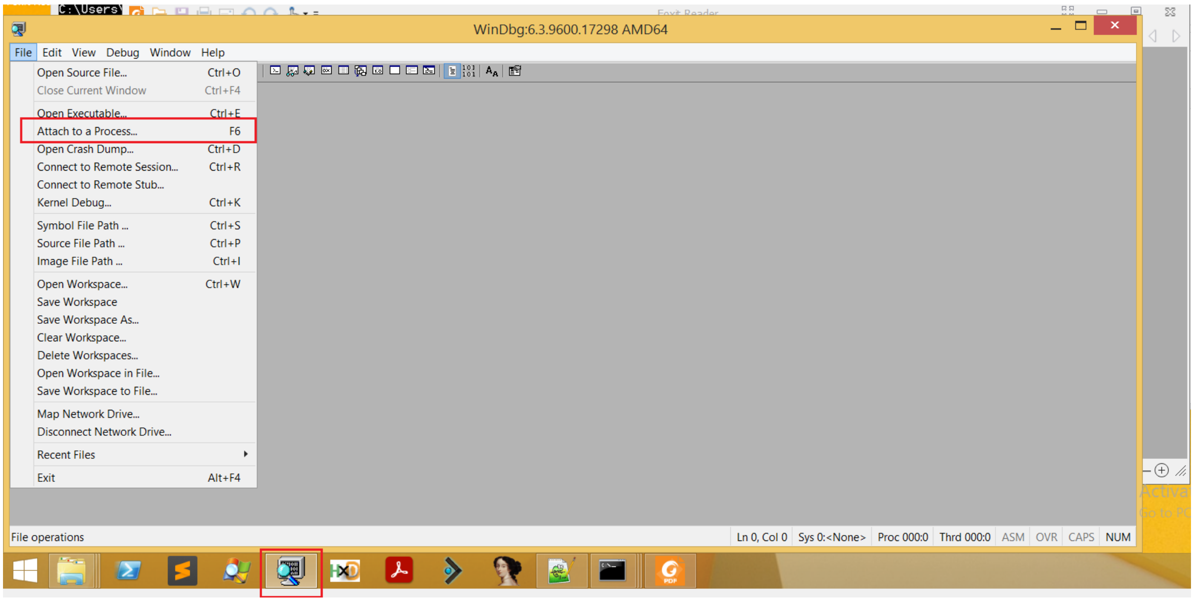
C:\Users\wxy\TypeOracle

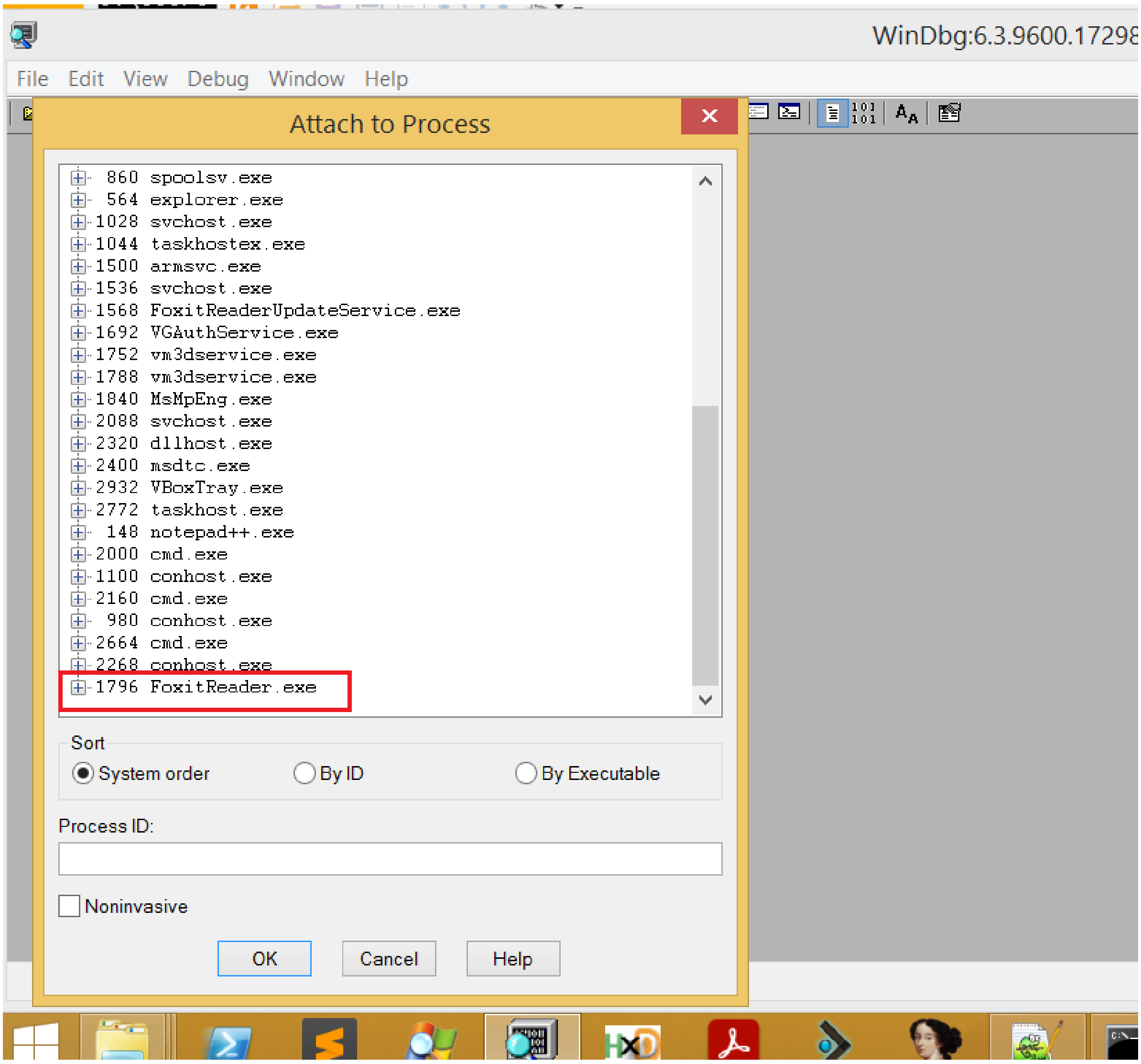
2. turn on the Page Heap

```
"C:\Program Files (x86)\Windows Kits\8.1\Debuggers\x86\gflags.exe" /p /enable
"C:\Program Files (x86)\Foxit Software\Foxit Reader\FoxitReader.exe"
```

3. open Foxit Reader, then open windbg.exe and attach to Foxit Reader (some vulnerabilities will be handled by the built-in exception handling mechanism of Foxit Reader, so that the program will not crash, but if we use windbg.exe to attach to Foxit Reader, windbg.exe will catch the exception instead of Foxit Reader)




WinDbg:6.3.9600.17298 AMD64
File
Edit
View
Debug
Window
Help
Open Source File... Ctrl+O
Close Current Window Ctrl+F4
Open Executable... Ctrl+E
Attach to a Process... F6
Open Crash Dump... Ctrl+D
Connect to Remote Session... Ctrl+R
Connect to Remote Stub...
Kernel Debug... Ctrl+K
Symbol File Path ... Ctrl+S
Source File Path ... Ctrl+P
Image File Path ... Ctrl+I
Open Workspace... Ctrl+W
Save Workspace
Save Workspace As...
Clear Workspace...
Delete Workspaces...
Open Workspace in File...
Save Workspace to File...
Map Network Drive...
Disconnect Network Drive...
Recent Files
Exit Alt+F4
File operations
Ln 0, Col 0
Sys 0:<None>
Proc 000:0
Thrd 000:0
ASM
OVR
CAPS
NUM



```
 860 spoolsv.exe
 564 explorer.exe
1028 svchost.exe
1044 taskhostex.exe
1500 armsvc.exe
1536 svchost.exe
1568 FoxitReaderUpdateService.exe
1692 VGAuthService.exe
1752 vm3dservice.exe
1788 vm3dservice.exe
1840 MsMpEng.exe
2088 svchost.exe
2320 dllhost.exe
2400 msdtc.exe
2932 VBoxTray.exe
2772 taskhost.exe
 148 notepad++.exe
2000 cmd.exe
1100 conhost.exe
2160 cmd.exe
 980 conhost.exe
2664 cmd.exe
2268 conhost.exe
1796 FoxitReader.exe
```

Sort

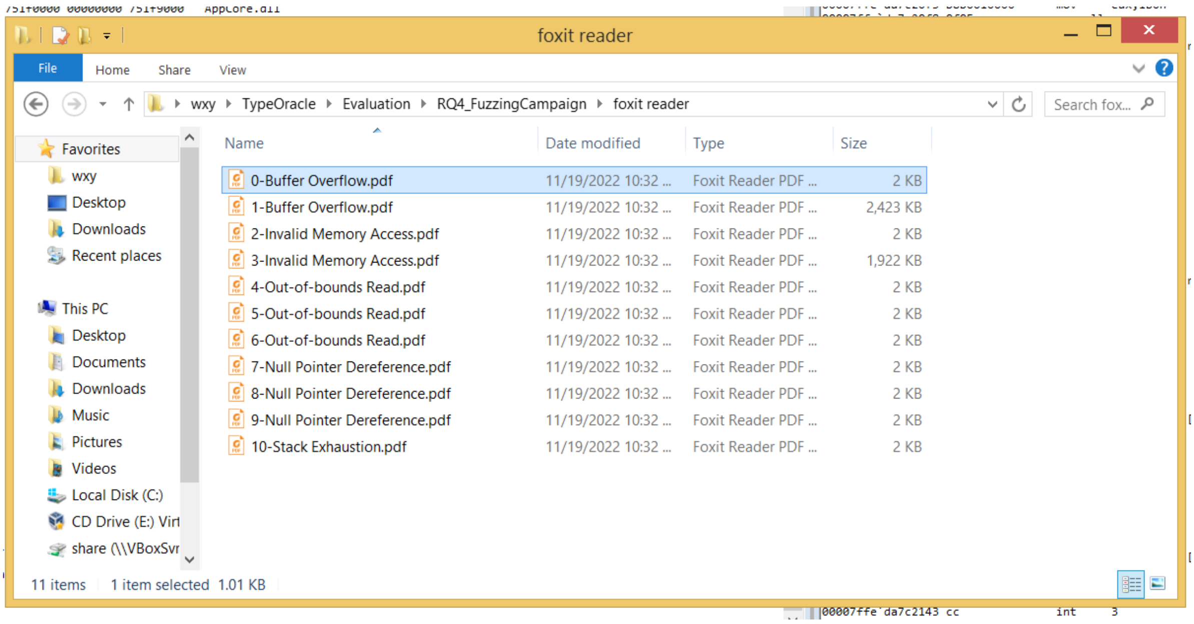
● System order ○ By ID ○ By Executable

Process ID:

□ Noninvasive

4. after the windbg attaches to Foxit Reader, press `F5` to continue

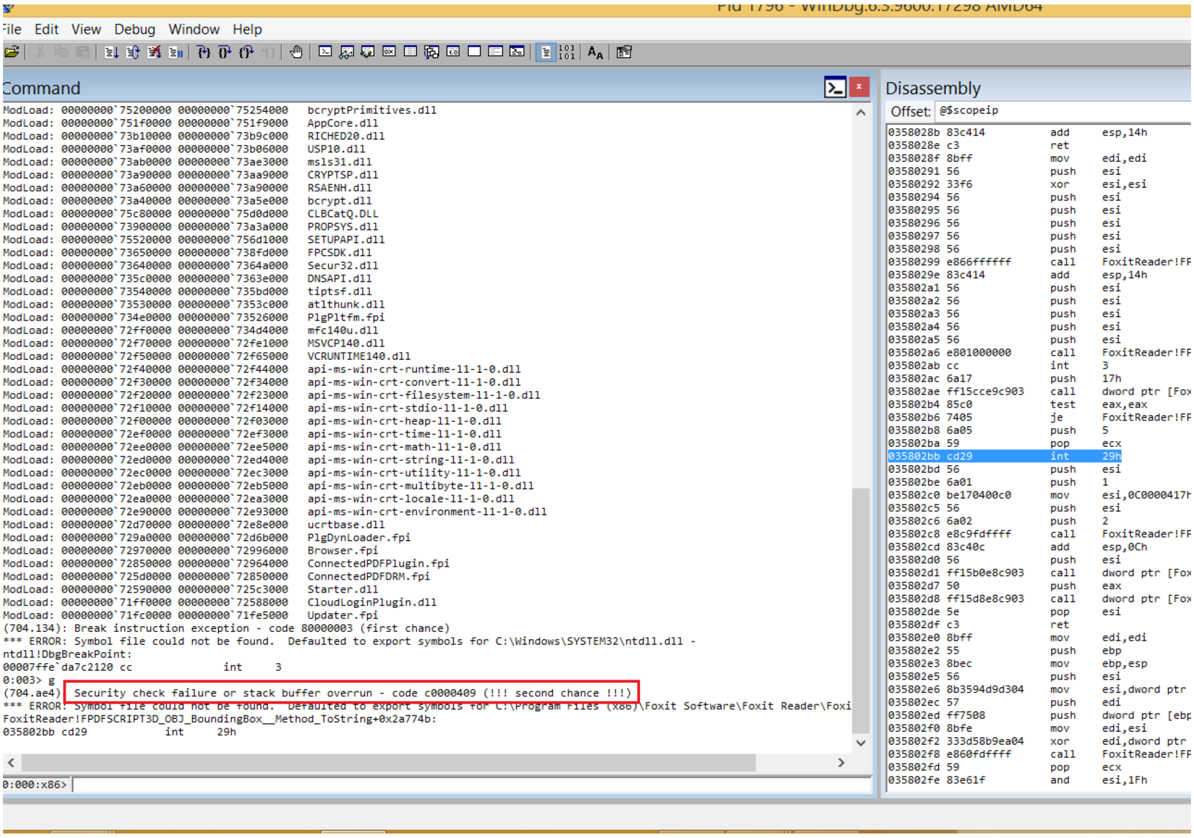
5. open any of them and windbg.exe will catch the exception



wxy › TypeOracle › Evaluation › RQ4_FuzzingCampaign › foxit reader

Name	Date modified	Type	Size
0-Buffer Overflow.pdf	11/19/2022 10:32 ...	Foxit Reader PDF ...	2 KB
1-Buffer Overflow.pdf	11/19/2022 10:32 ...	Foxit Reader PDF ...	2,423 KB
2-Invalid Memory Access.pdf	11/19/2022 10:32 ...	Foxit Reader PDF ...	2 KB
3-Invalid Memory Access.pdf	11/19/2022 10:32 ...	Foxit Reader PDF ...	1,922 KB
4-Out-of-bounds Read.pdf	11/19/2022 10:32 ...	Foxit Reader PDF ...	2 KB
5-Out-of-bounds Read.pdf	11/19/2022 10:32 ...	Foxit Reader PDF ...	2 KB
6-Out-of-bounds Read.pdf	11/19/2022 10:32 ...	Foxit Reader PDF ...	2 KB
7-Null Pointer Dereference.pdf	11/19/2022 10:32 ...	Foxit Reader PDF ...	2 KB
8-Null Pointer Dereference.pdf	11/19/2022 10:32 ...	Foxit Reader PDF ...	2 KB
9-Null Pointer Dereference.pdf	11/19/2022 10:32 ...	Foxit Reader PDF ...	2 KB
10-Stack Exhaustion.pdf	11/19/2022 10:32 ...	Foxit Reader PDF ...	2 KB

11 items 1 item selected 1.01 KB



```
ModLoad: 00000000`75200000 00000000`75254000   bcryptPrimitives.dll
ModLoad: 00000000`751f0000 00000000`751f9000   AppCore.dll
ModLoad: 00000000`73b10000 00000000`73b9c000   RICHED20.dll
ModLoad: 00000000`73af0000 00000000`73b06000   USP10.dll
ModLoad: 00000000`73ab0000 00000000`73ae3000   msls31.dll
ModLoad: 00000000`73a90000 00000000`73aa9000   CRYPTSP.dll
ModLoad: 00000000`73a60000 00000000`73a90000   RSAENH.dll
ModLoad: 00000000`73a40000 00000000`73a5e000   bcrypt.dll
ModLoad: 00000000`75c80000 00000000`75d0d000   CLBCatQ.DLL
ModLoad: 00000000`73900000 00000000`73a3a000   PROPSYS.dll
ModLoad: 00000000`75520000 00000000`756d1000   SETUPAPI.dll
ModLoad: 00000000`73650000 00000000`738fd000   FPCSDK.dll
ModLoad: 00000000`73640000 00000000`7364a000   Secur32.dll
ModLoad: 00000000`735c0000 00000000`7363e000   DNSAPI.dll
ModLoad: 00000000`73540000 00000000`735bd000   tiptsf.dll
ModLoad: 00000000`73530000 00000000`7353c000   atlthunk.dll
ModLoad: 00000000`734e0000 00000000`73526000   PlgPltfm.fpi
ModLoad: 00000000`72ff0000 00000000`734d4000   mfc140u.dll
ModLoad: 00000000`72f70000 00000000`72fe1000   MSVCP140.dll
ModLoad: 00000000`72f50000 00000000`72f65000   VCRUNTIME140.dll
ModLoad: 00000000`72f40000 00000000`72f44000   api-ms-win-crt-runtime-l1-1-0.dll
ModLoad: 00000000`72f30000 00000000`72f34000   api-ms-win-crt-convert-l1-1-0.dll
ModLoad: 00000000`72f20000 00000000`72f23000   api-ms-win-crt-filesystem-l1-1-0.dll
ModLoad: 00000000`72f10000 00000000`72f14000   api-ms-win-crt-stdio-l1-1-0.dll
ModLoad: 00000000`72f00000 00000000`72f03000   api-ms-win-crt-heap-l1-1-0.dll
ModLoad: 00000000`72ef0000 00000000`72ef3000   api-ms-win-crt-time-l1-1-0.dll
ModLoad: 00000000`72ee0000 00000000`72ee5000   api-ms-win-crt-math-l1-1-0.dll
ModLoad: 00000000`72ed0000 00000000`72ed4000   api-ms-win-crt-string-l1-1-0.dll
ModLoad: 00000000`72ec0000 00000000`72ec3000   api-ms-win-crt-utility-l1-1-0.dll
ModLoad: 00000000`72eb0000 00000000`72eb5000   api-ms-win-crt-multibyte-l1-1-0.dll
ModLoad: 00000000`72ea0000 00000000`72ea3000   api-ms-win-crt-locale-l1-1-0.dll
ModLoad: 00000000`72e90000 00000000`72e93000   api-ms-win-crt-environment-l1-1-0.dll
ModLoad: 00000000`72d70000 00000000`72e8e000   ucrtbase.dll
ModLoad: 00000000`729a0000 00000000`72d6b000   PlgDynLoader.fpi
ModLoad: 00000000`72970000 00000000`72996000   Browser.fpi
ModLoad: 00000000`72850000 00000000`72964000   ConnectedPDFPlugin.fpi
ModLoad: 00000000`725d0000 00000000`72850000   ConnectedPDFDRM.fpi
ModLoad: 00000000`72590000 00000000`725c3000   Starter.dll
ModLoad: 00000000`71ff0000 00000000`72588000   CloudLoginPlugin.dll
ModLoad: 00000000`71fc0000 00000000`71fe5000   Updater.fpi
(704.134): Break instruction exception - code 80000003 (first chance)
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for C:\Windows\SYSTEM32\ntdll.dll -
ntdll!DbgBreakPoint:
00007ffe`da7c2120 cc              int     3
0:003> g
(704.ae4)  Security check failure or stack buffer overrun - code c0000409 (!!! second chance !!!)
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for C:\Program Files (x86)\Foxit Software\Foxit Reader\Foxi
FoxitReader!FPDFSCRIPT3D_OBJ_BoundingBox__Method_ToString+0x2a774b:
035802bb cd29            int     29h

0:000:x86>
```

```
@$scopeip
0358028b 83c414          add     esp,14h
0358028e c3              ret
0358028f 8bff            mov     edi,edi
03580291 56              push    esi
03580292 33f6            xor     esi,esi
03580294 56              push    esi
03580295 56              push    esi
03580296 56              push    esi
03580297 56              push    esi
03580298 56              push    esi
03580299 e866ffffff      call    FoxitReader!FF
0358029e 83c414          add     esp,14h
035802a1 56              push    esi
035802a2 56              push    esi
035802a3 56              push    esi
035802a4 56              push    esi
035802a5 56              push    esi
035802a6 e801000000      call    FoxitReader!FF
035802ab cc              int     3
035802ac 6a17            push    17h
035802ae ff15cce9c903    call    dword ptr [Fox
035802b4 85c0            test    eax,eax
035802b6 7405            je      FoxitReader!FF
035802b8 6a05            push    5
035802ba 59              pop     ecx
035802bb cd29            int     29h
035802bd 56              push    esi
035802be 6a01            push    1
035802c0 be170400c0      mov     esi,0C0000417h
035802c5 56              push    esi
035802c6 6a02            push    2
035802c8 e8c9fdffff      call    FoxitReader!FF
035802cd 83c40c          add     esp,0Ch
035802d0 56              push    esi
035802d1 ff15b0e8c903    call    dword ptr [Fox
035802d7 50              push    eax
035802d8 ff15d8e8c903    call    dword ptr [Fox
035802de 5e              pop     esi
035802df c3              ret
035802e0 8bff            mov     edi,edi
035802e2 55              push    ebp
035802e3 8bec            mov     ebp,esp
035802e5 56              push    esi
035802e6 8b3594d9d304    mov     esi,dword ptr
035802ec 57              push    edi
035802ed ff7508          push    dword ptr [ebp
035802f0 8bfe            mov     edi,esi
035802f2 333d58b9ea04    xor     edi,dword ptr
035802f8 e860fdffff      call    FoxitReader!FF
035802fd 59              pop     ecx
035802fe 83e61f          and     esi,1Fh
```