

Penetration Testing Lab

Articles from the Pentesting Field

[Home](#)[Pentesting Distros](#)[Resources](#)[Submissions](#)[Toolkit](#)[Contact the Lab](#)[Privilege Escalation Methods – Poll](#)[UAC Bypass – Event Viewer](#)

Search the Lab



April 24,
2017

Windows Kernel Exploits



netbiosX
Windows



Privilege Escalation
5 Comments



Kernel, Local Exploits, Patches, Vulnerabilities,

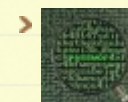
Windows by default are vulnerable to several vulnerabilities that could allow an attacker to execute malicious code in order to abuse a system. From the other side patching systems sufficiently is one of the main problems in security. Even if an organization has a patching policy in place if important patches are not implemented immediately this can still give short window to an attacker to exploit a vulnerability and escalate his privileges inside a system and therefore inside the network.

This article will discuss how to identify missing patches related to privilege escalation and the necessary code to exploit the issue.

Discovery of Missing Patches

The discovery of missing patches can be identified easily either through manual methods or automatic. Manually this can be done easily by executing the following command which

Author



netbiosX

Follow PenTest Lab

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

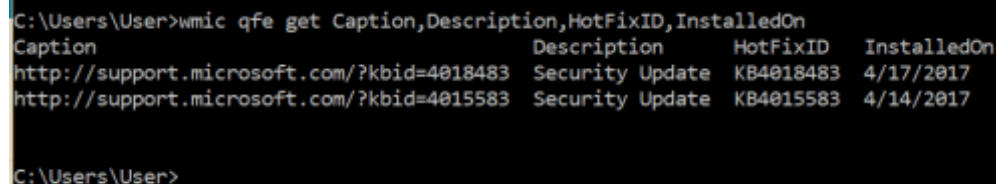
Join 1,640 other followers

[Follow](#)

will enumerate all the installed patches.

```
1 wmic qfe get Caption,Description,HotFixID,InstalledOn
```

The output will be similar to this:



Caption	Description	HotFixID	InstalledOn
http://support.microsoft.com/?kbid=4018483	Security Update	KB4018483	4/17/2017
http://support.microsoft.com/?kbid=4015583	Security Update	KB4015583	4/14/2017

Enumeration of Installed Patches

The HotFixID can be used in correlation with the table below in order to discover any missing patches related to privilege escalation. As the focus is on privilege escalation the command can be modified slightly to discover patches based on the KB number.

```
1 wmic qfe get Caption,Description,HotFixID,InstalledOn | finds
```

Alternatively this can be done automatically via Metasploit, Credential Nessus Scan or via a custom script that will look for missing patches related to privilege escalation.

Metasploit

There is a Metasploit module which can quickly identify any missing patches based on the Knowledge Base number and specifically patches for which there is a Metasploit module.

```
1 post/windows/gather/enum_patches
```

Recent Posts

- [PDF – NTLM Hashes](#)
- [NBNS Spoofing](#)
- [Lateral Movement – RDP](#)
- [DCShadow](#)
- [Skeleton Key](#)

Categories

- [Coding](#) (10)
- [Defense Evasion](#) (19)
- [Exploitation Techniques](#) (19)
- [External Submissions](#) (3)
- [General Lab Notes](#) (21)
- [Information Gathering](#) (12)
- [Infrastructure](#) (2)
- [Maintaining Access](#) (4)
- [Mobile Pentesting](#) (7)
- [Network Mapping](#) (1)
- [Post Exploitation](#) (11)
- [Privilege Escalation](#) (14)
- [Red Team](#) (24)
- [Social Engineering](#) (11)
- [Tools](#) (7)
- [VoIP](#) (4)
- [Web Application](#) (14)
- [Wireless](#) (2)

Archives

```

msf exploit(handler) > use post/windows/gather/enum_patches
msf post(enum_patches) > set SESSION 1
SESSION => 1
msf post(enum_patches) > set KB "KB3143141","KB3136041"
KB => KB3143141,KB3136041
msf post(enum_patches) > run

[+] KB3143141 is missing
[+] KB3136041 is missing
[+] KB977165 - Possibly vulnerable to MS10-015 kitrap0d if Windows 2K SP4 - Wind
ows 7 (x86)
[+] KB2305420 - Possibly vulnerable to MS10-092 schelevator if Vista, 7, and 200
8
[+] KB2592799 - Possibly vulnerable to MS11-080 afdjoinleaf if XP SP2/SP3 Win 2k
3 SP2
[+] KB2778930 - Possibly vulnerable to MS13-005 hwnd_broadcast, elevates from Lo
w to Medium integrity
[+] KB2850851 - Possibly vulnerable to MS13-053 schlamperei if x86 Win7 SP0/SP1
[+] KB2870008 - Possibly vulnerable to MS13-081 track_popup_menu if x86 Windows
7 SP0/SP1
[*] Post module execution completed

```

Metasploit – Patches Enumeration

Windows Exploit Suggester

Gotham Digital Security released a tool with the name Windows Exploit Suggester which compares the patch level of a system against the Microsoft vulnerability database and can be used to identify those exploits that could lead to privilege escalation. The only requirement is that requires the system information from the target.

- > May 2018
- > 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


```

root@kali:~/Desktop# ./windows-exploit-suggester.py --database 2017-04-23-mssb.x
ls --systeminfo windows2008R2-systeminfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 2 hotfix(es) against the 407 potential bulletins(s) with a dat
abase of 137 known exploits
[*] there are now 407 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2008 R2 SP1 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Import
ant
[*] https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - w
in32k Denial of Service (MS16-135)
[*] https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - '
win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*] https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Import
ant

```

Windows Exploit Suggester

PowerShell

There is also a PowerShell script which target to identify patches that can lead to privilege escalation. This script is called [Sherlock](#) and it will check a system for the following:

- MS10-015 : User Mode to Ring (KiTrap0D)
- MS10-092 : Task Scheduler
- MS13-053 : NTUserMessageCall Win32k Kernel Pool Overflow
- MS13-081 : TrackPopupMenuEx Win32k NULL Page
- MS14-058 : TrackPopupMenu Win32k Null Pointer Dereference
- MS15-051 : ClientCopyImage Win32k
- MS15-078 : Font Driver Buffer Overflow
- MS16-016 : 'mrxdav.sys' WebDAV
- MS16-032 : Secondary Logon Handle

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

@ Twitter

- [New Post] PDF - NTLM Hashes
[pentestlab.blog/2018/05/09/pdf... #pentestlab](#)
#Badpdf 3 hours ago
- Hiding Metasploit Shellcode to Evade Windows Defender [blog.rapid7.com/2018/05/03/hid...](#)
5 hours ago
- @CheckPointSW @InQuest I have a post scheduled ready for tomorrow regarding Bad-PDF. Really cool research! Great advantage dor red teams. **20 hours ago**
- [New Post] NBNS Spoofing
[pentestlab.blog/2018/05/08/nbn... #pentestlab](#)
#pentest 1 day ago
- RT @InQuest: From bad-PDF, [github.com/deepzec/Bad-Pdf](#), to worse-PDF, [github.com/3gstudent/Wors...](#), this YARA rule [github.com/InQuest/yara-r...](#) should co...
1 day ago

 Follow @netbiosX

Pen Test Lab Stats

- 2,950,921 hits

- CVE-2017-7199 : Nessus Agent 6.6.2 – 6.10.3 Priv Esc

The output of this tool can be seen below:

```
PS C:\Users\User> Find-AllVulns

Title      : User Mode to Ring (KiTrap0D)
MSBulletin : MS10-015
CVEID      : 2010-0232
Link       : https://www.exploit-db.com/exploits/11199/
VulnStatus : Not supported on 64-bit systems

Title      : Task Scheduler .XML
MSBulletin : MS10-092
CVEID      : 2010-3338, 2010-3888
Link       : https://www.exploit-db.com/exploits/19930/
VulnStatus : Not Vulnerable

Title      : NTUserMessageCall Win32k Kernel Pool Overflow
MSBulletin : MS13-053
CVEID      : 2013-1300
Link       : https://www.exploit-db.com/exploits/33213/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenuEx Win32k NULL Page
MSBulletin : MS13-081
CVEID      : 2013-3881
Link       : https://www.exploit-db.com/exploits/31576/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin : MS14-058
CVEID      : 2014-4113
Link       : https://www.exploit-db.com/exploits/35101/
VulnStatus : Appears Vulnerable
```

Sherlock – Missing Patches

Blogroll

- **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

```
Title      : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin : MS14-058
CVEID      : 2014-4113
Link       : https://www.exploit-db.com/exploits/35101/
UlnStatus  : Appears Vulnerable
```

```
Title      : ClientCopyImage Win32k
MSBulletin : MS15-051
CVEID      : 2015-1701, 2015-2433
Link       : https://www.exploit-db.com/exploits/37367/
UlnStatus  : Appears Vulnerable
```

```
Title      : Font Driver Buffer Overflow
MSBulletin : MS15-078
CVEID      : 2015-2426, 2015-2433
Link       : https://www.exploit-db.com/exploits/38222/
UlnStatus  : Not Vulnerable
```

```
Title      : 'mrxdav.sys' WebDAV
MSBulletin : MS16-016
CVEID      : 2016-0051
Link       : https://www.exploit-db.com/exploits/40085/
UlnStatus  : Not supported on 64-bit systems
```

```
Title      : Secondary Logon Handle
MSBulletin : MS16-032
CVEID      : 2016-0099
Link       : https://www.exploit-db.com/exploits/39719/
UlnStatus  : Appears Vulnerable
```

Sherlock – Identification of Privilege Escalation Patches

Privilege Escalation Table

The following table has been compiled to assist in the process of privilege escalation due to lack of sufficient patching.

Operating System	Description	Security Bulletin	KB	Exploit
Windows Server 2016	Windows Kernel Mode Drivers	MS16-135	3199135	Exploit Github

➤ **Irongeek** Hacking Videos,Infosec Articles,Scripts 0

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

Windows Server 2008 ,7,8,10 Windows Server 2012	Secondary Logon Handle	<u>MS16-032</u>	3143141	<u>GitHub</u> <u>ExploitDB</u> <u>Metasploit</u>	Advertisements
Windows Server 2008, Vista, 7	WebDAV	<u>MS16-016</u>	3136041	<u>Github</u>	
Windows Server 2003, Windows Server 2008, Windows 7, Windows 8, Windows 2012	Windows Kernel Mode Drivers	<u>MS15-051</u>	3057191	<u>GitHub</u> <u>ExploitDB</u> <u>Metasploit</u>	
Windows Server 2003, Windows Server 2008, Windows Server 2012, 7, 8	Win32k.sys	<u>MS14-058</u>	3000061	<u>GitHub</u> <u>ExploitDB</u> <u>Metasploit</u>	
Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012	AFD Driver	<u>MS14-040</u>	2975684	<u>Python</u> <u>EXE</u> <u>ExploitDB</u> <u>Github</u>	
Windows XP, Windows Server 2003	Windows Kernel	<u>MS14-002</u>	2914368	<u>Metasploit</u>	
Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012	Kernel Mode Driver	<u>MS13-005</u>	2778930	<u>Metasploit</u> <u>ExploitDB</u> <u>GitHub</u>	

Windows Server 2008, 7	Task Scheduler	<u>MS10-092</u>	2305420	<u>Metasploit</u> <u>ExploitDB</u>
Windows Server 2003, Windows Server 2008, 7, XP	KiTrap0D	<u>MS10-015</u>	977165	<u>Exploit</u> <u>ExploitDB</u> <u>GitHub</u> <u>Metasploit</u>
Windows Server 2003, XP	NDProxy	<u>MS14-002</u>	2914368	<u>Exploit</u> <u>ExploitDB</u> <u>ExploitDB</u> <u>Github</u>
Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012	Kernel Driver	<u>MS15-061</u>	3057839	<u>Github</u>
Windows Server 2003, XP	AFD.sys	<u>MS11-080</u>	2592799	<u>EXE</u> <u>Metasploit</u> <u>ExploitDB</u>
Windows Server 2003, XP	NDISTAPI	<u>MS11-062</u>	2566454	<u>ExploitDB</u>
Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012	RPC	<u>MS15-076</u>	3067505	<u>Github</u>
Windows Server 2003, Windows	Hot Potato	<u>MS16-</u>	3164038	<u>GitHub</u>

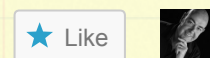
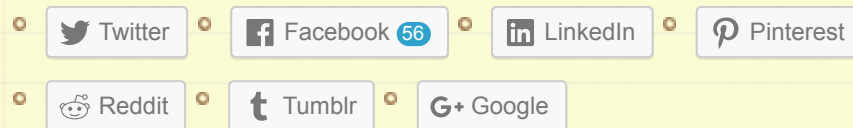
Server 2008, 7, 8, Windows Server 2012		<u>075</u>		<u>PowerShell</u> <u>HotPotato</u>
Windows Server 2003, Windows Server 2008, 7, XP	Kernel Driver	<u>MS15-010</u>	3036220	<u>GitHub</u> <u>ExploitDB</u>
Windows Server 2003, Windows Server 2008, 7, XP	AFD.sys	<u>MS11-046</u>	2503665	<u>EXE</u> <u>ExploitDB</u>

Advertisements

Rate this:



Share this:



One blogger likes this.

Related

Java Exploit Attack
(CVE-2012-0507)
In "Exploitation
Techniques"

Intel SYSRET
In "Privilege Escalation"

Windows Tools For
Penetration Testing
In "General Lab Notes"

5 Comments *(+add yours?)*



net

Apr 25, 2017 @ 11:38:11

this is so helpful i wish you can add linux exploit too 😊

👤 REPLY



netbiosX

Apr 25, 2017 @ 11:41:40

Thank you! I am planning to do the same at some point for Unix systems as well.

REPLY

Windows提权思路总结 – MoKirinSec

Apr 27, 2017 @ 08:37:21

半月安全看看看2017第六期 – 安全0day

Apr 28, 2017 @ 10:38:12

Windows privilege escalation – /dayvan-blog

May 24, 2017 @ 21:32:53

Leave a Reply

Enter your comment here...



Privilege Escalation Methods – Poll

UAC Bypass – Event Viewer



Blog at WordPress.com.

