

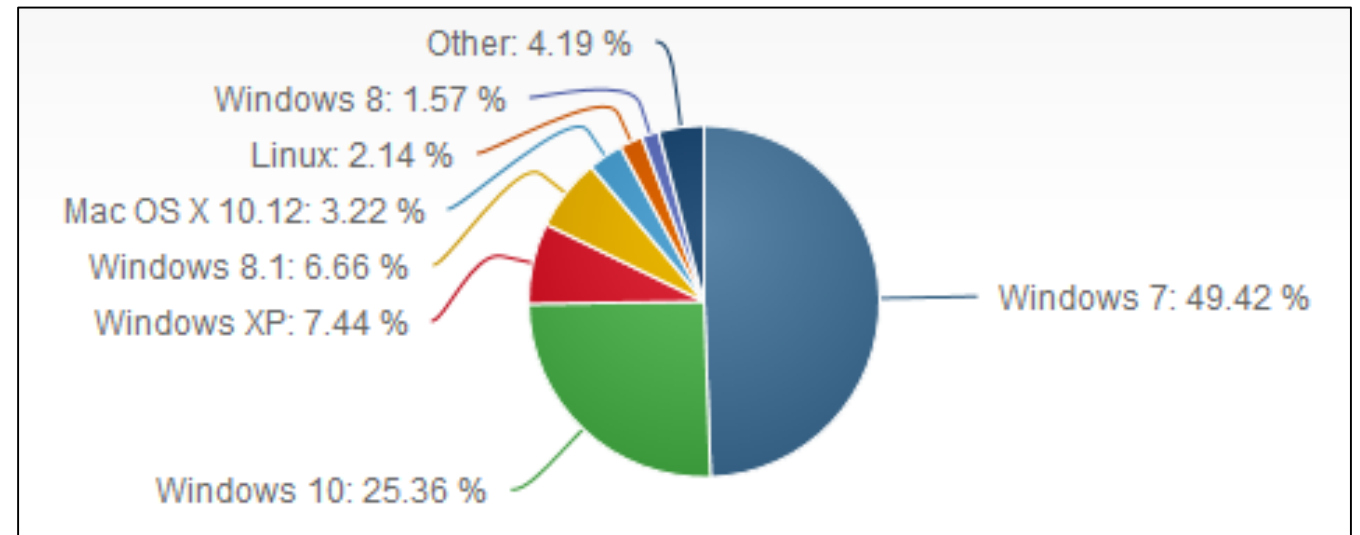
Microsoft Patch Analysis for Exploitation

Stephen Sims



OS Market Share

- Windows 7 clearly dominant
- XP still at 7.4%
- ATM Machines
- Embedded systems
- Windows 10 quickly gaining traction
- Mac OS and Linux still a small number in comparison



Taken on April 29th, 2017 from <https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustommd=0>

Application and OS Patching

- Maintaining a handle on the patching of a large number of systems and applications is complex
- The more users who have Administrative access to their workstations, the more likely there are going to be unique applications installed
 - Many of which are likely not approved
 - Some companies grant all users Administrative access to their computers
- Some vendors make patching easy, such as Microsoft, and others have no process at all
- Solutions like application whitelisting can be performed, but is hard when scaling in medium to large organizations

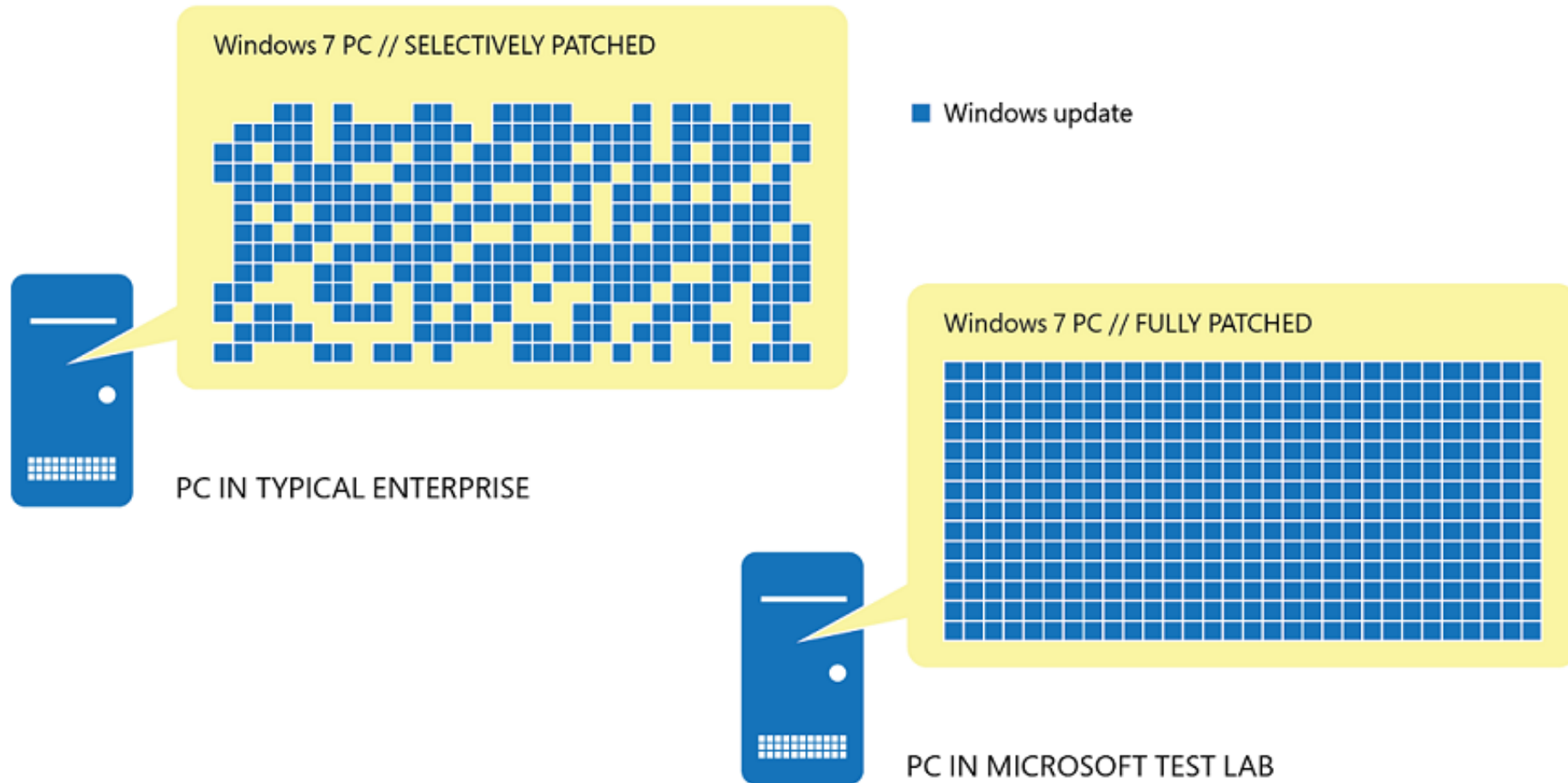
Microsoft Patch Tuesday

- Microsoft releases patches on the second Tuesday of each month, for now..., and only sometimes (No Feb, 2017 Patches...)
- An effort to help simplify the patching process
 - Random patch releases caused many users to miss patches
 - However, waiting up to 30 days for the next patch has security concerns
- Emergency patches are released out-of-cycle
- Exploits sometimes released in the days following
 - “One-Day Exploits”
 - Some vendors will buy exploits for patched privately disclosed vulnerabilities

Windows as a Service (WaaS)

- Windows has always had various versions (Professional , Home, Enterprise, Ultimate), service packs, monthly updates, etc...
- Microsoft desires to have all systems in the same known state
 - This allows them to perform QA testing on systems in the same state as the customers receiving updates
 - Monthly cumulative updates supersede the prior month's update and includes all features and fixes
 - Feature updates are deployed multiple times per year
 - Quality updates, including security patches, are sent in monthly cumulative packages
- Windows 10, Windows 10 Mobile, and Windows 10 IOT Mobile all fall under WaaS

Typical Patched System in an Enterprise vs. Microsoft Lab



<https://docs.microsoft.com/en-us/windows/deployment/update/waas-overview>

WaaS Servicing Branches

- Three servicing branches are available to allow organizations to choose when devices are updated
- Current Branch (CB) – Feature updates are immediately available to systems set not to defer updates
 - Good for developers and other groups to test for compatibility issues
- Current Branch for Business (CBB) – Updates deferred for about four months while vetted by business partners and customers
 - After about four months the CB build is assumed
 - Quality updates can only be deferred for 30 days using Windows Update for Business, but up to 12 months with WSUS
- Long-Term Servicing Branch (LTSB) – Updates deferred for an average of 2-3 years as devices are specialized, such as cash machines, medical, and automotive

Patch Distribution

- Windows Update
 - Automatic Updates, available in the Control Panel
- Vista, 7, 8,10 and Server 2008/2012/2016
 - Automatic Updates has expanded functionality
- Windows Server Update Service (WSUS)
 - Enterprise patch management solution
 - Control over patch distribution
- Windows Update for Business (WUB) for Windows 10
- Third-party Patch Management Solutions

Reverse Engineering Updates

- It is important to know that good guys, bad guys, and those in-between often reverse engineer security updates
- Exploitation frameworks such as Metasploit, Core Impact, SAINT Exploit, and Immunity Canvas want to be able to offer their customers exploits that are not available by their competitors
- Attackers want to quickly discover the patched vulnerability and attempt to develop a working exploit before most organizations patch
- The above is often referred to as a “1-day exploit” since there is a race condition between the time a patch is released and the time systems are patched
- Reversing patches is an acquired skill and is not limited to Microsoft updates

Obtaining Patches for Analysis Up Until April, 2017

<https://technet.microsoft.com/en-us/security/bulletins.aspx>

Microsoft Security Bulletin MS17-004 - Important

Security Update for Local Security Authority Subsystem Service

(3216771) ← Knowledge Base Number

Published: January 10, 2017

Version: 1.0

Executive Summary

A denial of service vulnerability exists in the way the Local Security Authority Subsystem Service (LSASS) handles authentication requests. An attacker who successfully exploited the vulnerability could cause a denial of service on the target system's LSASS service, which triggers an automatic reboot of the system.

This security update is rated Important for Microsoft Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 (and Server Core). For more information, see the **Affected Software and Vulnerability Severity Ratings** section.



On this page

[Executive Summary](#)

[Affected Software and Vulnerability Severity Ratings](#)

[Vulnerability Information](#)

[Security Update Deployment](#)

[Acknowledgments](#)



April, 2017's Update Changes Format Again...

- You must now go to: <https://portal.msrc.microsoft.com/en-us/security-guidance>
- More difficult to navigate
- You can still download the cumulative update from here
- You can get the actual vulnerability information here:
- <https://portal.msrc.microsoft.com/en-us/security-guidance/summary>

Security Update Guide

The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services, and provides the information here as part of the ongoing effort to help you manage security risks and help keep your systems protected.

Search by date range, product, severity, and impact; or search by KB or CVE number

From To All Product Categories All Products All Severities All Impacts

Search on CVE number or KB Article

Release Notes

Date	Release
04/11/2017	April 2017 Security Updates

Security Update [Download](#)

Show: Details Severity Impact Security Only

Date	More Info	Product	Platform
04/11/2017	4015219	Microsoft Edge	Windows 10 Version 1511 for 32-bit Systems
04/11/2017	4015219	Microsoft Edge	Windows 10 Version 1511 for x64-based Systems
04/11/2017	4015217	Microsoft Edge	Windows 10 Version 1607 for x64-based Systems
04/11/2017	4015217	Microsoft Edge	Windows 10 Version 1607 for 32-bit Systems

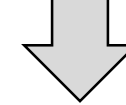
Types of Patches

- Patches for XP and Windows 2000, and 2003 server had .exe extensions, and still do for extended embedded XP support
 - For example, WindowsXP-KB979559-x86-ENU.exe
- Patches for Vista, 7, 8, 10, and Server 2008/2012/2016 have .msu extensions
 - For example, Windows6.0-KB979559-x86.msu
- Extraction methods differ slightly, as to the contents of each package

Extraction Tool for .msu Patches

- `expand -F:* <.msu file> <dest>`

Update File



```
c:\derp\MS16-106\Patched>expand -F:* Windows6.1-KB3185911-x86.msu .  
Microsoft (R) File Expansion Utility Version 6.1.7600.16385  
Copyright (c) Microsoft Corporation. All rights reserved.
```

```
Adding .\WSUSSCAN.cab to Extraction Queue
```

```
Adding .\Windows6.1-KB3185911-x86.cab to Extraction Queue
```

```
Adding .\Windows6.1-KB3185911-x86-pkgProperties.txt to Extraction Queue
```

```
Adding .\Windows6.1-KB3185911-x86.xml to Extraction Queue
```

```
Expanding Files ....
```

```
Expanding Files Complete ...
```

```
4 files total.
```

Cabinet File Contents

- We are interested in .cab files

```
c:\derp\MS16-106\Patched>expand -F:* Windows6.1-KB3185911-x86.cab .
```

#Output truncated for space...

```
c:\derp\MS16-106\Patched>dir /s /b /o:n /ad
```

```
c:\derp\MS16-106\Patched\x86_microsoft-windows-user32_31bf3856ad364e35_6.1.7601.23528_none_cfc274bde4coef6f
```

```
c:\derp\MS16-106\Patched\x86_microsoft-windows-win32k_31bf3856ad364e35_6.1.7601.23528_none_bb7d823711eb39fd
```



We can see that one directory contains a patch to user32.dll and the other win32k.sys

The Patched File

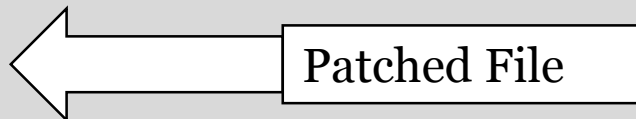
- Examining folder contents

```
c:\derp\MS16-106\Patched>cd x86_microsoft-windows-user32_31bf3856ad364e35_6.1.7601.23528_none_cfc274bde4coef6f
```

```
c:\derp\MS16-106\Patched\x86_microsoft-windows-user32_31bf3856ad364e35_6.1.7601.23528_none_cfc274bde4coef6f>dir
Volume in drive C has no label.
Volume Serial Number is CEF2-482A
```

```
Directory of c:\derp\MS16-106\Patched\x86_microsoft-windows-user32_31bf3856ad364e35_6.1.7601.23528_none_cfc274bde4coef6f
```

```
01/31/2017 12:57 PM <DIR>      .
01/31/2017 12:57 PM <DIR>      ..
08/15/2016 06:48 PM          811,520 user32.dll
    1 File(s)      811,520 bytes
    2 Dir(s) 161,884,778,496 bytes free
```

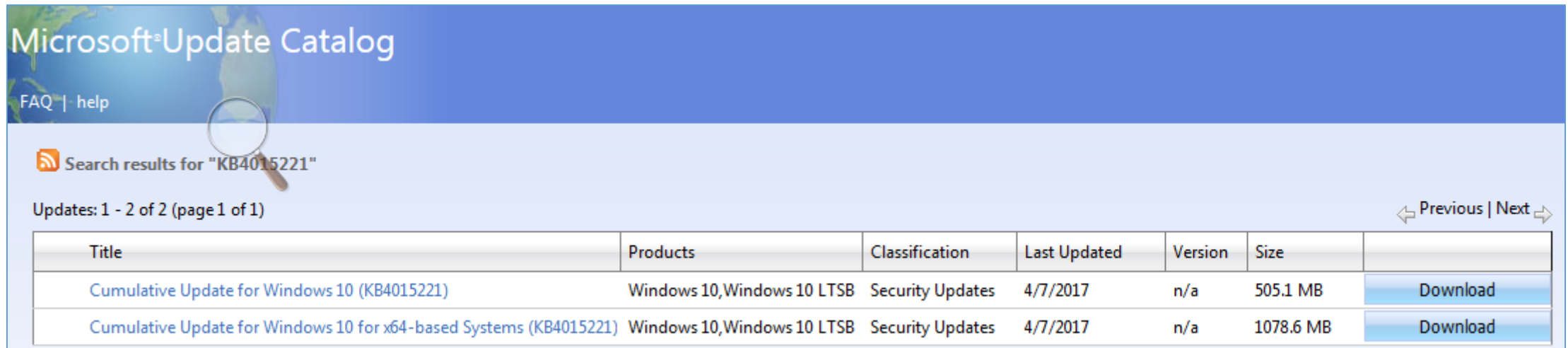


Extracting Cumulative Updates

- As mentioned previously, patches are now cumulative and contain all updates for the OS version
- This *can* make for very large update files that contain hundreds of files
- Mapping an extracted file to the right Knowledge Base (KB) number is difficult
- Greg Linares (@Laughing_Mantis) wrote some PowerShell scripts to help with this problem
 - The concept is quite simple, using the modified data on the updates to identify files that have changed within the last 30 days
 - They are then placed into unique directories and cleanup is performed
 - You still need to determine which file correlates to which advisory, but the process is much easier

Obtaining a Cumulative Update for Windows 10

- The following screenshot shows the cumulative update file for April, 2017



Microsoft® Update Catalog

FAQ | help

Search results for "KB4015221"

Updates: 1 - 2 of 2 (page 1 of 1) Previous | Next

Title	Products	Classification	Last Updated	Version	Size	
Cumulative Update for Windows 10 (KB4015221)	Windows 10, Windows 10 LTSB	Security Updates	4/7/2017	n/a	505.1 MB	Download
Cumulative Update for Windows 10 for x64-based Systems (KB4015221)	Windows 10, Windows 10 LTSB	Security Updates	4/7/2017	n/a	1078.6 MB	Download

...but, Window 7's update is just around 100mb

Very large files

PatchExtract

- Now that we have the updated downloaded, let's extract it with PatchExtract13 from Greg Linares

```
c:\Patches\MS17-JAN\x86>Powershell -ExecutionPolicy Bypass -File c:\Patches\PatchExtract13.ps1 -Patch windows10.0-kb3210720-x86_04faf73b558f6796b73c2fff144256122f4e36a9.msu -Path c:\Patches\MS17-JAN
```

- The above command looks quite long, but much of that is due to the long .msu filename
- This command took ~10 minutes to complete on the 500MB file
- It extracted every folder and file from the cumulative update and resulted in an enormous number of folders
- When randomly looking at a couple of the modified dates on some patched files, many dated all the way back to 2015

PatchClean

- We will now clean up the enormous output and list only the files changed within the past 30 days

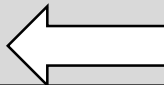
```
c:\Patches\MS17-JAN\x86> Powershell -ExecutionPolicy Bypass -File c:\Patches\PatchClean.ps1 -Path c:\Patches\MS17-JAN\x86\
```

#Lots of output that has been truncated for space...

```
=====  
Low Priority Folders: 1020
```

```
Low Priority Files: 3810
```

```
High Priority Folders: 16
```



- As you can see, PatchClean has identified 16 folders whose contents have changed within the last 30 days
- This saves us a TON of time!

PatchExtract / PatchClean Demonstration

- Extracting the April, 2017 Update



Patch Extraction Results

```
Administrator: Command Prompt
c:\Patches\MS17-JAN\x86>dir
Volume in drive C has no label.
Volume Serial Number is 6681-3E06

Directory of c:\Patches\MS17-JAN\x86

01/10/2017  05:38 PM      <DIR>      .
01/10/2017  05:38 PM      <DIR>      ..
01/10/2017  04:47 PM      <DIR>      b..ironment-dvd-efisys_10.0.10240.17236
01/10/2017  05:01 PM      <DIR>      b..re-bootmanager-pcat_10.0.10240.17236
01/10/2017  05:01 PM      <DIR>      b..re-memorydiagnostic_10.0.10240.17236
01/10/2017  05:01 PM      <DIR>      b..vironment-os-loader_10.0.10240.17236
01/10/2017  04:49 PM      <DIR>      gdi32_10.0.10240.17236
01/10/2017  04:48 PM      <DIR>      i..ia-mergedcomponents_10.0.10240.17236
01/10/2017  05:01 PM      <DIR>      ie-htmlrendering_11.0.10240.17236
01/10/2017  04:48 PM      <DIR>      ntprint.inf_10.0.10240.17236
01/10/2017  05:01 PM      <DIR>      ntprint4.inf_10.0.10240.17184
01/10/2017  05:01 PM      <DIR>      OLD
01/10/2017  05:38 PM      283 Powershell
01/10/2017  04:48 PM      <DIR>      prnms003.inf_10.0.10240.17236
01/10/2017  05:01 PM      <DIR>      prnms004.inf_10.0.10240.17236
01/10/2017  04:47 PM      <DIR>      s..-spp-plugin-windows_10.0.10240.17236
01/10/2017  04:48 PM      <DIR>      s..y-spp-plugin-common_10.0.10240.17236
01/10/2017  05:01 PM      <DIR>      scripting-jscript9_11.0.10240.17236
01/10/2017  04:48 PM      <DIR>      winpe-smi-schema_10.0.10240.17236
01/10/2017  05:01 PM      <DIR>      xusb22.inf_10.0.10240.17146

          1 File(s)          283 bytes
         19 Dir(s)  45,534,920,704 bytes free
```

Mapping a Patched File to the Security Advisory

- MS17-001 says:

Microsoft Security Bulletin MS17-001 - Important

Security Update for Microsoft Edge (3214288)

Published: January 10, 2017

```
c:\Patches\MS17-JAN\x86>cd ie-htmlrendering_11.0.10240.17236
```

```
c:\Patches\MS17-JAN\x86\ie-htmlrendering_11.0.10240.17236>dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 6681-3E06
```

```
Directory of c:\Patches\MS17-JAN\x86\ie-htmlrendering_11.0.10240.17236
```

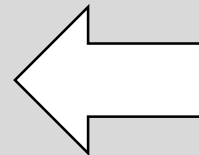
```
01/10/2017 05:01 PM <DIR> .
```

```
01/10/2017 05:01 PM <DIR> ..
```

```
12/21/2016 12:00 AM 18,796,032 edgehtml.dll
```

```
1 File(s) 18,796,032 bytes
```

```
2 Dir(s) 45,532,430,336 bytes free
```



Patch Diffing

- Security patches are often made to applications, DLLs, driver files, and shared objects
- When a new version is released, it can be difficult to locate what changes were made
 - Some are new features or general application changes
 - Some are security fixes
 - Some changes are intentional to thwart reversing
- Some vendors make it clear as to reasoning for the update to the binary
- Binary diffing tools can help you locate the changes

Binary Diffing Tools

- The following is a list of well-known binary diffing tools:
 - **Zynamics/Google's BinDiff**: Free as of March 18, 2016!
 - **Core Security's turbodiff**: Free
 - **DarunGrim 4 by Jeongwook Oh**: Free
 - **patchdiff2 by Nicolas Pouvesle**: Free
 - **Diaphora** by Joxean Koret
 - There are more

Example of BinDiff Results

The screenshot shows the zynamics BinDiff application window titled "_LoadAnilcon@20 vs _LoadAnilcon@20 - zynamics BinDiff". The interface includes a menu bar (View, Mode, Graphs, Selection, Search, Window, Help) and a toolbar with various icons for navigation and analysis. The main workspace displays a control flow graph (CFG) on the left and right sides, with assembly code snippets in the center. The assembly code is color-coded: green for identical instructions and red for differences. A large, semi-transparent watermark reading "primary" is overlaid on the left side of the workspace.

Left Panel Address List:

- 77D64FE
- 77D64FF
- 77D6500
- 77D6501
- 77D6502
- 77D6503
- 77D6504
- 77D6505
- 77D6506

Right Panel Address List:

- 77D64FA
- 77D64FB
- 77D64FD
- 77D64FE
- 77D64FF
- 77D6500
- 77D6501
- 77D6502

Assembly Code Snippets:

Top Left (77D653B8):

```
77D653B8 push    eax
77D653B9 push    ebx
77D653BA call   ebx
77D653BB call   ebx
77D653BC mov    eax, ebx
77D653BD jmp    77D653D4
```

Top Right (77D65375):

```
77D65375 push    eax
77D65376 push    ebx
77D65377 call   ebx
77D65378 call   ebx
77D65379 mov    eax, ebx
77D6537A jmp    77D6537A
```

Middle Left (77D65388):

```
77D65388 mov    eax, ebx
77D65389 and    eax, ebx
77D6538A and    eax, ebx
77D6538B push    eax
77D6538C mov    eax, ebx
77D6538D pop    eax
77D6538E int3
77D6538F and    eax, ebx
77D65390 and    ebx, eax
77D65391 and    ebx, eax
77D65392 and    ebx, eax
77D65393 and    ebx, eax
77D65394 and    ebx, eax
```

Middle Right (77D65375):

```
77D65375 mov    eax, ebx
77D65376 and    eax, ebx
77D65377 and    eax, ebx
77D65378 push    eax
77D65379 mov    eax, ebx
77D6537A pop    eax
77D6537B int3
77D6537C and    ebx, eax
77D6537D and    ebx, eax
77D6537E and    ebx, eax
77D6537F and    ebx, eax
77D65380 and    ebx, eax
77D65381 and    ebx, eax
77D65382 and    ebx, eax
77D65383 and    ebx, eax
77D65384 and    ebx, eax
```

Bottom Left (77D65388):

```
77D65388 int3
77D65389 push    eax
77D6538A push    ebx
77D6538B call   ebx
77D6538C call   ebx
77D6538D call   ebx
77D6538E jmp    77D6538E
```

Bottom Right (77D65375):

```
77D65375 int3
77D65376 push    eax
77D65377 push    ebx
77D65378 call   ebx
77D65379 call   ebx
77D6537A jmp    77D6537A
```

Example of a Patched Vulnerability – MS16-009

```
0000000018003B2A0 ?BuildUserAgentStringMobileHelper@@YAPEADW4UACOMPATMODE@@PEADW4USERAGENT_TYPE@@H@Z
0000000018003BDA1 xor     r8d, r8d           // dwFlags
0000000018003BDA4 lea    b8 rcx, b8 cs:[LibFileName] // LibFileName

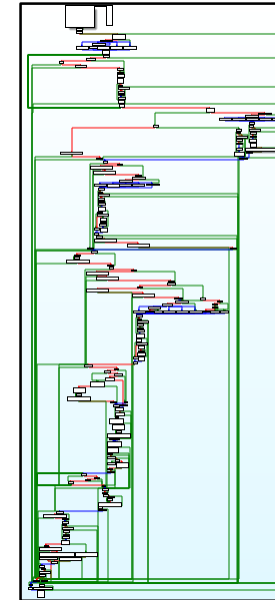
0000000018003BDAB xor     edx, edx           // hFile
0000000018003BDAD call   b8 cs:[__imp_LoadLibraryExW] // __imp_LoadLibraryExW
0000000018003BDB3 test   b8 rax, b8 rax
0000000018003BDB6 jz     b8 loc_18003BE7B
```

Unpatched

```
0000000018003B2A0 ?BuildUserAgentStringMobileHelper@@YAPEADW4UACOMPATMODE@@PEADW4USERAGENT_TYPE@@H@Z
0000000018003BCB1 xor     edx, edx           // hFile
0000000018003BCB3 lea    b8 rcx, b8 cs:[LibFileName] // LibFileName
0000000018003BCBA mov     r8d, 0x800        // dwFlags

0000000018003BCC0 call   b8 cs:[__imp_LoadLibraryExW] // __imp_LoadLibraryExW
0000000018003BCC6 test   b8 rax, b8 rax
0000000018003BCC9 jz     b8 loc_18003BD8C
```

Patched



MSI6-009 Demonstration



- Critical SMB vulnerabilities disclosed
- Patch Tuesday in February delayed until March

Windows SMB Information Disclosure Vulnerability – CVE-2017-0147

An information disclosure vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited this vulnerability could craft a special packet, which could lead to information disclosure from the server.

To exploit the vulnerability, in most situations, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv1 server.

The security update addresses the vulnerability by correcting how SMBv1 handles these specially crafted requests.

The following table contains links to the standard entry for each vulnerability in the Common Vulnerabilities and Exposures list:

Vulnerability title	CVE number	Publicly disclosed	Exploited
Windows SMB Information Disclosure Vulnerability	CVE-2017-0147	No	No

MSI7-010 BinDiff Demo



An oldie but goodie...

- If we have time, a quick demo of an older and simple, but very clear vulnerability in MS07-017...



Thanks!

Stephen Sims

@Steph3nSims

stephen@deadlisting.com

The recorded presentation is available at:

<https://www.youtube.com/watch?v=LHNcBVQF1tM>

<http://www.irongeek.com/i.php?page=videos/bsidescharm2017/bsidescharm-2017-t111-microsoft-patch-analysis-for-exploitation-stephen-sims>