Scan Report

November 11, 2015

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "bobbyscan". The scan started at Wed Nov 11 18:44:08 2015 UTC and ended at Wed Nov 11 19:00:54 2015 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.25 blackyfox-1.home	46	14	1	48	0
Total: 1	46	14	1	48	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.

This report contains all 109 results selected by the filtering described above. Before filtering there were 109 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.1.25 - blackyfox-1.home	SMB	Success	Protocol SMB, Port 445, User bobby

2 Results per Host

2.1 192.168.1.25

Host scan start	Wed Nov 11 18:44:19 2015 UTC
Host scan end	Wed Nov 11 19:00:53 2015 UTC

Service (Port)	Threat Level
general/tcp	High
general/tcp	Medium
135/tcp	Medium
general/tcp	Low
general/tcp	Log
general/CPE-T	Log
2869/tcp	Log
139/tcp	Log
445/tcp	Log
general/SMBClient	Log
554/tcp	Log

2.1.1 High general/tcp

High (CVSS: 9.3)
NVT: Microsoft Sidebar and Gadgets Remote Code Execution Vulnerability (2719662)

Summary
This host is installed with Microsoft Windows Sidebar and Gadgets and is prone to remote code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote attackers to execute arbitrary code as the logged-on user. Impact Level: System/Application

Solution
Apply the Patch from below links, http://technet.microsoft.com/en-us/security/advisory/2719662

Affected Software/OS
Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
Windows Sidebar when running insecure Gadgets allows an attacker to run arbitrary code.

Vulnerability Detection Method
Details:`Microsoft Sidebar and Gadgets Remote Code Execution Vulnerability (2719662)`
OID:1.3.6.1.4.1.25623.1.0.802886
Version used: `$Revision: 12 $`

References
```
Other:
  URL:http://support.microsoft.com/kb/2719662
   URL:http://technet.microsoft.com/en-us/security/advisory/2719662
```

High (CVSS: 9.3)
NVT: Microsoft Unauthorized Digital Certificates Spoofing Vulnerability (2728973)

Summary
This host is installed with Microsoft Windows operating system and is prone to Spoofing vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

. . . continues on next page . . .

... continued from previous page ...

Impact
Successful exploitation could allow remote attackers to use the certificates to spoof content, perform phishing attacks, or perform man-in-the-middle attacks. Impact Level: System

Solution
Apply the Patch from below link, http://support.microsoft.com/kb/2728973

Affected Software/OS
Microsoft Windows XP x32 Edition Service Pack 3 and prior Microsoft Windows XP x64 Edition Service Pack 2 and prior Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
Microsoft certificate authorities, which are stored outside the recommended secure storage practices can be misused. An attacker could use these certificates to spoof content, perform phishing attacks, or perform man-in-the-middle attacks.

Vulnerability Detection Method
Details:`Microsoft Unauthorized Digital Certificates Spoofing Vulnerability (2728973)`
OID:1.3.6.1.4.1.25623.1.0.802912
Version used: `$Revision: 12 $`

References
```
Other:
  URL:http://support.microsoft.com/kb/2728973
   URL:http://technet.microsoft.com/en-us/security/advisory/2728973
```

High (CVSS: 9.3)
NVT: Microsoft Office Word Remote Code Execution Vulnerabilities (2949660)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS14-017.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute the arbitrary code, cause memory corruption and compromise the system.
Impact Level: System/Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-017

Affected Software/OS
Microsoft Word 2013 Microsoft Word 2003 Service Pack 3 and prior Microsoft Word 2007 Service Pack 3 and prior Microsoft Word 2010 Service Pack 2 and prior.

Vulnerability Insight
Multiple flaws are due to an error within, - Microsoft Word when handling certain RTF-formatted data can be exploited to corrupt memory. - Microsoft Office File Format Converter when handling certain files can be exploited to corrupt memory. - Microsoft Word when handling certain files can be exploited to cause a stack-based buffer overflow.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Word Remote Code Execution Vulnerabilities (2949660)`
OID:1.3.6.1.4.1.25623.1.0.804423
Version used: `$Revision: 1559 $`

References
```
CVE: CVE-2014-1757, CVE-2014-1758, CVE-2014-1761
BID:66385, 66614, 66629
Other:
  URL:https://support.microsoft.com/kb/2878303
   URL:https://support.microsoft.com/kb/2878237
   URL:https://support.microsoft.com/kb/2863926
   URL:https://support.microsoft.com/kb/2863910
   URL:http://technet.microsoft.com/en-us/security/bulletin/ms14-017
```

High (CVSS: 9.3)
NVT: Microsoft Office Remote Code Execution Vulnerabilities (2961037)

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-023.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute the arbitrary code.
Impact Level: System/Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-023

Affected Software/OS
Microsoft Office 2007 Service Pack 3 (proofing tools) Microsoft Office 2010 Service Pack 2 (proofing tools) and prior Microsoft Office 2013 Service Pack 1 (proofing tools) and prior

Vulnerability Insight
- The flaw is due to the Grammar Checker feature for Chinese (Simplified) loading libraries in an insecure manner. - An error when handling a certain response can be exploited to gain knowledge of access tokens used for authentication of the current user.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Remote Code Execution Vulnerabilities (2961037)`
OID:1.3.6.1.4.1.25623.1.0.804450
Version used: `$Revision: 1559 $`

References
```
CVE: CVE-2014-1756, CVE-2014-1808
BID:67274, 67279
Other:
  URL:https://support.microsoft.com/kb/2767772
   URL:https://support.microsoft.com/kb/2878284
   URL:https://support.microsoft.com/kb/2878316
   URL:https://technet.microsoft.com/en-us/security/bulletin/ms14-023
```

High (CVSS: 9.3)
NVT: Microsoft Office Remote Code Execution Vulnerability (3017349)

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-082.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code on the affected system.
Impact Level: System/Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-082

Affected Software/OS
Microsoft Office 2007 Service Pack 3 and prior Microsoft Office 2010 Service Pack 2 and prior Microsoft Office 2013 Service Pack 1 and prior.

Vulnerability Insight
The flaw is due to a use-after-free error and can be exploited to corrupt memory.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Remote Code Execution Vulnerability (3017349)`
OID:1.3.6.1.4.1.25623.1.0.805022
Version used: `$Revision: 1559 $`

References
`CVE: CVE-2014-6364`
`BID:71474`
`Other:`
`URL:http://secunia.com/advisories/61150`
`URL:https://support.microsoft.com/kb/3017349`
`URL:https://technet.microsoft.com/library/security/ms14-082`

High (CVSS: 9.3)
NVT: Microsoft Office Excel Remote Code Execution Vulnerabilities (3017347)

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-083.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code on the affected system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-083

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Microsoft Excel 2013 Microsoft Excel 2007 Service Pack 3 and prior Microsoft Excel 2010 Service Pack 2 and prior

Vulnerability Insight
Flaws are due to, - An error related to a global free which can be exploited to corrupt memory. - An error related to an invalid pointer which can be exploited to corrupt memory.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Excel Remote Code Execution Vulnerabilities (3017347)`
OID:1.3.6.1.4.1.25623.1.0.805023
Version used: `$Revision: 1559 $`

References
`CVE: CVE-2014-6360, CVE-2014-6361`
`BID:71500, 71501`
`Other:`
`URL:http://secunia.com/advisories/61151`
`URL:https://support.microsoft.com/kb/3017347`
`URL:https://technet.microsoft.com/en-us/security/bulletin/ms14-083`

High (CVSS: 9.3)
NVT: Microsoft Office Word Remote Code Execution Vulnerabilities (3017301)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS14-081.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute the arbitrary code, cause memory corruption and compromise the system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS14-081

Affected Software/OS
Microsoft Word 2007 SP3 and prior Microsoft Word 2010 Service Pack 2 and prior Microsoft Word 2013 Service Pack 1 and prior

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaws are due to, - An invalid indexing error when parsing Office files can be exploited to execute arbitrary code via a specially crafted Office file. - A use-after-free error when parsing Office files can be exploited to execute arbitrary code via a specially crafted Office file.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Word Remote Code Execution Vulnerabilities (3017301)`
OID:1.3.6.1.4.1.25623.1.0.805025
Version used: `$Revision: 1559 $`

References
`CVE: CVE-2014-6356, CVE-2014-6357`
`BID:71469, 71470`
`Other:`
`URL:http://secunia.com/advisories/61149`
`URL:https://support.microsoft.com/kb/3017301`
`URL:https://technet.microsoft.com/library/security/MS14-081`

High (CVSS: 9.3)
NVT: Microsoft Office Excel Remote Code Execution Vulnerability (3032328)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-012.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code on the affected system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms15-012

Affected Software/OS
Microsoft Excel 2013 Microsoft Excel 2007 Service Pack 3 and prior Microsoft Excel 2010 Service Pack 2 and prior

Vulnerability Insight
A remote code execution vulnerability exists in Microsoft Excel that is caused when Excel improperly handles objects in memory while parsing specially crafted Office files.

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Excel Remote Code Execution Vulnerability (3032328)`
OID:1.3.6.1.4.1.25623.1.0.805042
Version used: `$Revision: 1005 $`

References
`CVE: CVE-2015-0063`
`BID:72460`
`Other:`
`URL:https://support.microsoft.com/kb/3032328`
`URL:https://support.microsoft.com/kb/2920753`
`URL:https://support.microsoft.com/kb/2920788`
`URL:https://support.microsoft.com/kb/2956081`
`URL:https://technet.microsoft.com/en-us/security/bulletin/ms15-012`

High (CVSS: 9.3)
NVT: Microsoft Office Suite Remote Code Execution Vulnerabilities (3038999)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-022.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms15-022

Affected Software/OS
Microsoft Office 2007 Service Pack 3 and prior Microsoft Office 2010 Service Pack 2 and prior Microsoft Office 2013 Service Pack 1 and prior.

Vulnerability Insight
Multiple flaws are exists when, - The Office software improperly handles objects in memory while parsing specially crafted Office files. - The Office software fails to properly handle rich text format files in memory.

Vulnerability Detection Method

. . . continues on next page . . .

... continued from previous page ...

Get the vulnerable file version and check appropriate patch is applied or not.
Details:Microsoft Office Suite Remote Code Execution Vulnerabilities (3038999)
OID:1.3.6.1.4.1.25623.1.0.805054
Version used: $Revision: 1076 $

References
CVE: CVE-2015-0085, CVE-2015-0086, CVE-2015-0097
Other:
URL:http://support.microsoft.com/kb/2984939
URL:http://support.microsoft.com/kb/2956151
URL:http://support.microsoft.com/kb/2956076
URL:http://support.microsoft.com/kb/2889839
URL:http://support.microsoft.com/kb/2883100
URL:http://support.microsoft.com/kb/2956138
URL:https://technet.microsoft.com/library/security/ms15-022

High (CVSS: 9.3)
NVT: Microsoft Office Word Remote Code Execution Vulnerabilities (3038999)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-022.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms15-022

Affected Software/OS
Microsoft Word 2010, Microsoft Word 2013 and Microsoft Word 2007 Service Pack 3 and prior

Vulnerability Insight
Multiple flaws are exists when, - The Office software improperly handles objects in memory while parsing specially crafted Office files. - The Office software fails to properly handle rich text format files in memory.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.

... continues on next page ...

... continued from previous page ...

Details:Microsoft Office Word Remote Code Execution Vulnerabilities (3038999)
OID:1.3.6.1.4.1.25623.1.0.805057
Version used: $Revision: 1076 $

References
CVE: CVE-2015-0085, CVE-2015-0086, CVE-2015-0097
Other:
URL:http://support.microsoft.com/kb/2956163
URL:http://support.microsoft.com/kb/2956139
URL:http://support.microsoft.com/kb/2956109
URL:https://technet.microsoft.com/library/security/ms15-022

High (CVSS: 9.3)
NVT: Microsoft Office Word Remote Code Execution Vulnerabilities (3048019)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-033.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms15-033

Affected Software/OS
Microsoft Word 2010, Microsoft Word 2013 and Microsoft Word 2007 Service Pack 3 and prior.

Vulnerability Insight
Multiple flaws are exists when, - The Office software improperly handles objects in memory while parsing specially crafted Office files. - The Office software fails to properly handle rich text format files in memory.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:Microsoft Office Word Remote Code Execution Vulnerabilities (3048019)
OID:1.3.6.1.4.1.25623.1.0.805062
Version used: $Revision: 1165 $

... continues on next page ...

... continued from previous page ...

References

CVE: CVE-2015-1641, CVE-2015-1650, CVE-2015-1649, CVE-2015-1651
Other:
URL:https://support.microsoft.com/en-us/kb/2965284
URL:https://support.microsoft.com/en-us/kb/2965224
URL:https://support.microsoft.com/en-us/kb/2553428
URL:https://technet.microsoft.com/library/security/ms15-033

High (CVSS: 9.3)
NVT: Microsoft Office Suite Remote Code Execution Vulnerabilities (3064949)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-059.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow a context-dependent attacker to corrupt memory and potentially execute arbitrary code.
Impact Level: System/Application

Solution

Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-059

Affected Software/OS

Microsoft Office 2010 Service Pack 2 and prior Microsoft Office 2013 Service Pack 1 and prior.

Vulnerability Insight

Flaw exists as user supplied input is not properly validated.

Vulnerability Detection Method

Get the vulnerable file version and check appropriate patch is applied or not.
Details:Microsoft Office Suite Remote Code Execution Vulnerabilities (3064949)
OID:1.3.6.1.4.1.25623.1.0.805069
Version used: $Revision: 1327 $

References

CVE: CVE-2015-1759, CVE-2015-1760, CVE-2015-1770
BID:75014, 75015, 75016
Other:
URL:https://support.microsoft.com/en-us/kb/3064949
URL:https://technet.microsoft.com/library/security/MS15-059

High (CVSS: 9.3)
NVT: Microsoft Graphics Component Remote Code Executioon Vulnerabilities (3078662)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-080.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code. Failed exploit attempts will result in a denial-of-service condition.
Impact Level: System

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the given link, https://technet.microsoft.com/library/security/MS15-080

Affected Software/OS
Microsoft Windows 8 x32/x64 Microsoft Windows Server 2012/R2 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
The flaw is due to the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Graphics Component Remote Code Executioon Vulnerabilities (3078662)`
OID:1.3.6.1.4.1.25623.1.0.805081
Version used: `$Revision: 1563 $`

References
```
CVE: CVE-2015-2432, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461,
↪CVE-2015-2462, CVE-2015-2435, CVE-2015-2455, CVE-2015-2456, CVE-2015-2463, CVE
↪-2015-2464, CVE-2015-2433, CVE-2015-2453, CVE-2015-2454, CVE-2015-2465
Other:
  URL:https://support.microsoft.com/en-us/kb/3078662
   URL:https://technet.microsoft.com/library/security/MS15-080
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Remote Code Execution Vulnerabilities (3078662)

. . . continues on next page . . .

... continued from previous page ...

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-080.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow an attacker to gain access to potentially sensitive information and to execute arbitrary code on the affected system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-080

Affected Software/OS
Microsoft .NET Framework 3.0 Service Pack 2 Microsoft .NET Framework 3.5 Microsoft .NET Framework 3.5.1 Microsoft .NET Framework 4 Microsoft .NET Framework 4.5, 4.5.1, and 4.5.2, Microsoft .NET Framework 4.6 and 4.6 RC

Vulnerability Insight
The flaw exists due to improper handling of TrueType fonts and OpenType fonts.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft .NET Framework Remote Code Execution Vulnerabilities (3078662)`
OID:1.3.6.1.4.1.25623.1.0.805082
Version used: `$Revision: 1563 $`

References
```
CVE: CVE-2015-2460, CVE-2015-2462, CVE-2015-2455, CVE-2015-2456, CVE-2015-2463,
↪CVE-2015-2464
Other:
  URL:https://support.microsoft.com/en-us/kb/3078662
   URL:https://technet.microsoft.com/library/security/MS15-080
```

High (CVSS: 9.3)
NVT: Microsoft Office Suite Remote Code Execution Vulnerabilities (3080790)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-081.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow a context-dependent attacker to corrupt memory and potentially execute arbitrary code.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-081

Affected Software/OS
Microsoft Office 2007 Service Pack 3 and prior Microsoft Office 2010 Service Pack 2 and prior Microsoft Office 2013 Service Pack 1 and prior.

Vulnerability Insight
Flaws exist as user supplied input is not properly validated.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Suite Remote Code Execution Vulnerabilities (3080790)`
OID:1.3.6.1.4.1.25623.1.0.805087
Version used: `$Revision: 1563 $`

References
```
CVE: CVE-2015-1642, CVE-2015-2423, CVE-2015-2466, CVE-2015-2467, CVE-2015-2468,
↪CVE-2015-2469, CVE-2015-2470, CVE-2015-2477
Other:
  URL:https://support.microsoft.com/en-us/kb/2596650
   URL:https://support.microsoft.com/en-us/kb/2687409
   URL:https://support.microsoft.com/en-us/kb/2837610
   URL:https://support.microsoft.com/en-us/kb/3054888
   URL:https://support.microsoft.com/en-us/kb/2598244
   URL:https://technet.microsoft.com/library/security/MS15-081
```

High (CVSS: 9.3)
NVT: Microsoft Office Word Multiple Remote Code Execution Vulnerabilities (3080790)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-081.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.

... continues on next page ...

... continued from previous page ...

Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms15-081

Affected Software/OS
Microsoft Word 2007 Service Pack 3 and prior, Microsoft Word 2010 Service Pack 2 and prior, Microsoft Word 2013 Service Pack 1 and prior.

Vulnerability Insight
Flaws are due to improper handling of files in the memory.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Word Multiple Remote Code Execution Vulnerabilities (3080790)`
OID:1.3.6.1.4.1.25623.1.0.805090
Version used: `$Revision: 1563 $`

References
```
CVE: CVE-2015-2423, CVE-2015-2468, CVE-2015-2469
Other:
  URL:https://support.microsoft.com/en-us/kb/3055052
   URL:https://support.microsoft.com/en-us/kb/3055039
   URL:https://support.microsoft.com/en-us/kb/3055030
   URL:https://technet.microsoft.com/en-us/library/security/MS15-081
```

High (CVSS: 9.3)
NVT: Microsoft Office Suite Remote Code Execution Vulnerability (3057181)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-046.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow a context-dependent attacker to corrupt memory and potentially execute arbitrary code.
Impact Level: System/Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-046

Affected Software/OS
Microsoft Office 2007 Service Pack 3 and prior Microsoft Office 2010 Service Pack 2 and prior Microsoft Office 2013 Service Pack 1 and prior.

Vulnerability Insight
Flaw exists as user supplied input is not properly validated.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Suite Remote Code Execution Vulnerability (3057181)`
OID:1.3.6.1.4.1.25623.1.0.805180
Version used: `$Revision: 1233 $`

References
```
CVE: CVE-2015-1682, CVE-2015-1683
BID:74481, 74484
Other:
  URL:http://osvdb.org/122005
   URL:http://osvdb.org/122006
   URL:https://support.microsoft.com/en-us/kb/2965282
   URL:https://support.microsoft.com/en-us/kb/2965311
   URL:https://support.microsoft.com/en-us/kb/2999412
   URL:https://support.microsoft.com/en-us/kb/2965242
   URL:https://support.microsoft.com/en-us/kb/2975808
   URL:https://technet.microsoft.com/library/security/MS15-046
```

High (CVSS: 9.3)
NVT: Microsoft Office Excel Remote Code Execution Vulnerability (3057181)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-046.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow a context-dependent attacker to corrupt memory and potentially execute arbitrary code.
Impact Level: System/Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-046

Affected Software/OS
Microsoft Excel 2010 Service Pack 2 and prior, Microsoft Excel 2013 Service Pack 1 and prior.

Vulnerability Insight
Flaw exists as user supplied input is not properly validated.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Excel Remote Code Execution Vulnerability (3057181)`
OID:1.3.6.1.4.1.25623.1.0.805181
Version used: `$Revision: 1233 $`

References
```
CVE: CVE-2015-1682, CVE-2015-1683
BID:74481, 74484
Other:
  URL:http://osvdb.org/122005
   URL:http://osvdb.org/122006
   URL:https://support.microsoft.com/en-us/kb/2965240
   URL:https://support.microsoft.com/en-us/kb/2986216
   URL:https://technet.microsoft.com/library/security/MS15-046
```

High (CVSS: 9.3)
NVT: Microsoft Office PowerPoint Remote Code Execution Vulnerability (3057181)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-046.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow a context-dependent attacker to corrupt memory and potentially execute arbitrary code.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-046

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Microsoft PowerPoint 2010 Service Pack 2 and prior, Microsoft PowerPoint 2013 Service Pack 1 and prior.

Vulnerability Insight
Flaw exists as user supplied input is not properly validated.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office PowerPoint Remote Code Execution Vulnerability (3057181)`
OID:1.3.6.1.4.1.25623.1.0.805182
Version used: `$Revision: 1233 $`

References
```
CVE: CVE-2015-1682, CVE-2015-1683
BID:74481, 74484
Other:
  URL:http://osvdb.org/122005
   URL:http://osvdb.org/122006
   URL:https://support.microsoft.com/en-us/kb/2999420
   URL:https://support.microsoft.com/en-us/kb/2975816
   URL:https://technet.microsoft.com/library/security/MS15-046
```

High (CVSS: 9.3)
NVT: Microsoft Office Word Remote Code Execution Vulnerability (3057181)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-046.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow a context-dependent attacker to corrupt memory and potentially execute arbitrary code.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-046

Affected Software/OS
Microsoft Word 2010 Service Pack 2 and prior, Microsoft Word 2013 Service Pack 1 and prior.

Vulnerability Insight
Flaw exists as user supplied input is not properly validated.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Word Remote Code Execution Vulnerability (3057181)`
OID:1.3.6.1.4.1.25623.1.0.805183
Version used: `$Revision: 1233 $`

References
```
CVE: CVE-2015-1682, CVE-2015-1683
BID:74481, 74484
Other:
  URL:http://osvdb.org/122005
   URL:http://osvdb.org/122006
   URL:https://support.microsoft.com/en-us/kb/2965237
   URL:https://support.microsoft.com/en-us/kb/2965307
   URL:https://technet.microsoft.com/library/security/MS15-046
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (3082442)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-079.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to corrupt memory and potentially execute arbitrary code in the context of the current user.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the link, https://technet.microsoft.com/en-us/library/security/MS15-079

Affected Software/OS
Microsoft Internet Explorer version 7.x/8.x/9.x/10.x/11.x

Vulnerability Insight
Multiple flaws are due to, - Multiple improper handling memory objects, - Fails to use ASLR security feature, allowing an attacker to more reliably predict the memory offsets of specific instructions.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.

... continues on next page ...

... continued from previous page ...

Details:Microsoft Internet Explorer Multiple Vulnerabilities (3082442)
OID:1.3.6.1.4.1.25623.1.0.805731
Version used: $Revision: 1563 $

References

CVE: CVE-2015-2423, CVE-2015-2441, CVE-2015-2442, CVE-2015-2443, CVE-2015-2444, ↪CVE-2015-2445, CVE-2015-2446, CVE-2015-2447, CVE-2015-2448, CVE-2015-2449, CVE ↪-2015-2450, CVE-2015-2451, CVE-2015-2452
BID:76202, 76197, 76196, 76195, 76194, 76198, 76193, 76192, 76191, 76199, 76190, ↪ 76189, 76188
Other:
URL:https://support.microsoft.com/en-us/kb/3082442
URL:https://technet.microsoft.com/en-us/library/security/MS15-079

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (3089548)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-094.

Vulnerability Detection Result

File checked: C:\Windows\system32\Mshtml.dll
File version: 11.0.9600.17924
Vulnerable range: less than 11.0.9600.18036

Impact

Successful exploitation will allow remote attackers to corrupt memory and potentially execute arbitrary code in the context of the current user.
Impact Level: System/Application

Solution

Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the link, https://technet.microsoft.com/en-us/library/security/MS15-094

Affected Software/OS

Microsoft Internet Explorer version 7.x/8.x/9.x/10.x/11.x

Vulnerability Insight

Multiple flaws are due to, - Multiple improper handling memory objects, - Improper permissions validation, allowing a script to be run with elevated privileges.

Vulnerability Detection Method

Get the vulnerable file version and check appropriate patch is applied or not.
Details:Microsoft Internet Explorer Multiple Vulnerabilities (3089548)
OID:1.3.6.1.4.1.25623.1.0.805736

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 1689 $

References

CVE: CVE-2015-2483, CVE-2015-2484, CVE-2015-2485, CVE-2015-2486, CVE-2015-2487,
↪CVE-2015-2489, CVE-2015-2490, CVE-2015-2491, CVE-2015-2492, CVE-2015-2493, CVE
↪-2015-2494, CVE-2015-2498, CVE-2015-2499, CVE-2015-2500, CVE-2015-2501, CVE-20
↪15-2541, CVE-2015-2542
Other:
URL:https://support.microsoft.com/en-us/kb/3089548
URL:https://technet.microsoft.com/en-us/library/security/MS15-094

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer Multiple Vulnerabilities (3096441)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-106.

Vulnerability Detection Result

File checked: C:\Windows\system32\Mshtml.dll
File version: 11.0.9600.17924
Vulnerable range: 11.0.9600.00000 - 11.0.9600.18056

Impact

Successful exploitation will allow remote attackers to corrupt memory and potentially execute arbitrary code in the context of the current user.
Impact Level: System/Application

Solution

Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the link, https://technet.microsoft.com/en-us/library/security/MS15-106

Affected Software/OS

Microsoft Internet Explorer version 7.x/8.x/9.x/10.x/11.x

Vulnerability Insight

Multiple flaws are due to, - Multiple improper handling memory objects, - Improper permissions validation, allowing a script to be run with elevated privileges.

Vulnerability Detection Method

Get the vulnerable file version and check appropriate patch is applied or not.
Details:Microsoft Internet Explorer Multiple Vulnerabilities (3096441)
OID:1.3.6.1.4.1.25623.1.0.805761
Version used: $Revision: 1938 $

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2015-2482, CVE-2015-6042, CVE-2015-6044, CVE-2015-6046, CVE-2015-6047,
↪CVE-2015-6048, CVE-2015-6049, CVE-2015-6050, CVE-2015-6051, CVE-2015-6052, CVE
↪-2015-6053, CVE-2015-6055, CVE-2015-6056, CVE-2015-6059
Other:
URL:https://support.microsoft.com/en-us/kb/3096441
URL:https://technet.microsoft.com/en-us/library/security/MS15-106

High (CVSS: 9.3)
NVT: Microsoft Office Excel Multiple Remote Code Execution Vulnerabilities (3072620)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-070.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms15-070

Affected Software/OS
Microsoft Excel 2007 Service Pack 3 and prior, Microsoft Excel 2010 Service Pack 2 and prior, Microsoft Excel 2013 Service Pack 1 and prior.

Vulnerability Insight
Multiple flaws exists when, - Microsoft Excel improperly handles the loading of dynamic link library (DLL) files. - Error when memory is released in an unintended manner. - Improper handling of files in the memory.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:Microsoft Office Excel Multiple Remote Code Execution Vulnerabilities (3072620)
OID:1.3.6.1.4.1.25623.1.0.805809
Version used: $Revision: 1452 $

References
CVE: CVE-2015-2376, CVE-2015-2377, CVE-2015-2415, CVE-2015-2378, CVE-2015-2375
Other:
URL:https://support.microsoft.com/en-us/kb/2965281

... continues on next page ...

... continued from previous page ...

URL:https://support.microsoft.com/en-us/kb/3054981
URL:https://support.microsoft.com/en-us/kb/3054949
URL:https://technet.microsoft.com/en-us/library/security/MS15-070

High (CVSS: 9.3)
NVT: Microsoft Office PowerPoint Remote Code Execution Vulnerability (3072620)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-070.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms15-070

Affected Software/OS
Microsoft PowerPoint 2007 Service Pack 3 and prior, Microsoft PowerPoint 2010 Service Pack 2 and prior, Microsoft PowerPoint 2013 Service Pack 1 and prior.

Vulnerability Insight
Flaw is due to improper handling of files in the memory.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:Microsoft Office PowerPoint Remote Code Execution Vulnerability (3072620)
OID:1.3.6.1.4.1.25623.1.0.805810
Version used: $Revision: 1452 $

References
CVE: CVE-2015-2424
Other:
URL:https://support.microsoft.com/en-us/kb/2965283
URL:https://support.microsoft.com/en-us/kb/3054963
URL:https://support.microsoft.com/en-us/kb/3054999
URL:https://technet.microsoft.com/en-us/library/security/MS15-070

High (CVSS: 9.3)
NVT: Microsoft Office Word Mutiple Remote Code Execution Vulnerabilities (3072620)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-070.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms15-070

Affected Software/OS
Microsoft Word 2007 Service Pack 3 and prior, Microsoft Word 2010 Service Pack 2 and prior, Microsoft Word 2013 Service Pack 1 and prior.

Vulnerability Insight
Multiple flaws are due to improper handling of files in the memory.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Word Mutiple Remote Code Execution Vulnerabilities (3072620)`
OID:1.3.6.1.4.1.25623.1.0.805811
Version used: `$Revision: 1452 $`

References
```
CVE: CVE-2015-2379, CVE-2015-2380, CVE-2015-2424
Other:
  URL:https://support.microsoft.com/en-us/kb/3054996
   URL:https://support.microsoft.com/en-us/kb/3054973
   URL:https://support.microsoft.com/en-us/kb/3054990
   URL:https://technet.microsoft.com/en-us/library/security/MS15-070
```

High (CVSS: 9.3)
NVT: Microsoft Internet Explorer RCE vulnerability (3088903)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-093.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
File checked:     C:\Windows\system32\Mshtml.dll
File version:     11.0.9600.17924
Vulnerable range: 11.0.9600.00000 - 11.0.9600.17962
```

Impact

Successful exploitation will allow remote attackers to corrupt memory and potentially execute arbitrary code in the context of the current user.
Impact Level: System/Application

Solution

Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the link, https://technet.microsoft.com/en-us/library/security/MS15-093

Affected Software/OS

Microsoft Internet Explorer version 7.x/8.x/9.x/10.x/11.x

Vulnerability Insight

The error exists due to multiple improper handling of memory objects.

Vulnerability Detection Method

Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Internet Explorer RCE vulnerability (3088903)`
OID:1.3.6.1.4.1.25623.1.0.805959
Version used: `$Revision: 1689 $`

References

```
CVE: CVE-2015-2502
BID:76403
Other:
  URL:https://support.microsoft.com/kb/3088903
   URL:https://support.microsoft.com/kb/3087985
   URL:https://technet.microsoft.com/en-us/library/security/MS15-093
```

High (CVSS: 9.3)
NVT: Microsoft Windows Journal Remote Code Execution Vulnerability (3089669)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS15-098.

Vulnerability Detection Result

```
File checked:     C:\Program Files\Common Files\Microsoft Shared\ink\Journal.dll
File version:     6.1.7601.18815
Vulnerable range: Less than 6.1.7601.18951
```

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow remote attackers to conduct denial-of-service attack or execute arbitrary code and compromise a user's system.
Impact Level: System

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/ms15-098

Affected Software/OS
Microsoft Windows 10 x32/x64 Microsoft Windows 8/8.1 x32/x64 Microsoft Windows Server 2012/R2 Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
The flaw is due to an unspecified error within Windows Journal while parsing Journal files.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Windows Journal Remote Code Execution Vulnerability (3089669)`
OID:1.3.6.1.4.1.25623.1.0.805977
Version used: `$Revision: 1689 $`

References
```
CVE: CVE-2015-2513, CVE-2015-2514, CVE-2015-2516, CVE-2015-2519, CVE-2015-2530
Other:
  URL:https://support.microsoft.com/en-us/kb/3069114
   URL:https://support.microsoft.com/en-us/kb/3089669
   URL:https://technet.microsoft.com/library/security/ms15-098
```

High (CVSS: 9.3)
NVT: Microsoft .NET Framework Privilege Elevation Vulnerabilities (3089662)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-101.

Vulnerability Detection Result
```
File checked:     C:\Windows\Microsoft.NET\Framework64\v4.0.30319\System.Drawing
↪.dll
File version:     4.0.30319.18408
Vulnerable range: Less than 2.0.50727.5492
```

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow an attacker to conduct denial-of-service attack and take complete control of an affected system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/ms15-101

Affected Software/OS
Microsoft .NET Framework 2.0 Service Pack 2 Microsoft .NET Framework 3.5 Microsoft .NET Framework 3.5.1 Microsoft .NET Framework 4 Microsoft .NET Framework 4.5, 4.5.1, and 4.5.2, Microsoft .NET Framework 4.6 and 4.6 RC

Vulnerability Insight
Multiple flaws exists due to, - An unspecified error in the way that the .NET Framework validates the number of objects in memory before copying those objects into an array. - Application fails to properly handle certain specially crafted requests.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft .NET Framework Privilege Elevation Vulnerabilities (3089662)`
OID:1.3.6.1.4.1.25623.1.0.805978
Version used: `$Revision: 1689 $`

References
`CVE: CVE-2015-2504, CVE-2015-2526`
`Other:`
`URL:https://support.microsoft.com/en-us/kb/3089662`
`URL:https://technet.microsoft.com/library/security/ms15-101`

High (CVSS: 9.3)
NVT: Microsoft Windows Graphics Component Remote Code Execution Vulnerability (3089656)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-097.

Vulnerability Detection Result
```
File checked:     C:\Windows\system32\Win32k.sys
File version:     6.1.7601.18906
Vulnerable range: Less than 6.1.7601.18985
```

Impact
Successful exploitation will allow an attacker to do Kernel Address Space Layout Randomization (KASLR) bypass and execute arbitrary code taking complete control of the affected system.
Impact Level: System/Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/ms15-097

Affected Software/OS
Microsoft Windows 8/8.1 x32/x64 Microsoft Windows Server 2012/R2 Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior

Vulnerability Insight
Multiple flaws exists due to, - An unspecified error in the Windows Adobe Type Manager Library which improperly handles specially crafted OpenType fonts. - An unspecified error in Windows Adobe Type Manager Library which fails to properly handle objects in memory. - Multiple errors in Windows kernel-mode driver which fails to properly handle objects in memory. - An unspecified error in the Windows kernel mode driver (Win32k.sys) which fails to properly validate and enforce integrity levels during certain process initialization scenarios. - An error in Windows kernel which fails to properly initialize a memory address.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Windows Graphics Component Remote Code Execution Vulnerability (30896.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.805979
Version used: `$Revision: 1689 $`

References
```
CVE: CVE-2015-2506, CVE-2015-2507, CVE-2015-2508, CVE-2015-2510, CVE-2015-2511,
↪CVE-2015-2512, CVE-2015-2517, CVE-2015-2518, CVE-2015-2527, CVE-2015-2529, CVE
↪-2015-2546
Other:
  URL:https://support.microsoft.com/en-us/kb/3086255
   URL:https://support.microsoft.com/en-us/kb/3087039
   URL:https://support.microsoft.com/en-us/kb/3087135
   URL:https://technet.microsoft.com/library/security/ms15-097
```

High (CVSS: 9.3)
NVT: MS Windows Shell and Tablet Input Band Remote Code Execution Vulnerabilities (3096443)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-109.

Vulnerability Detection Result
`File checked:  C:\Windows\system32\Shell32.dll`

... continues on next page ...

... continued from previous page ...

```
File version:     6.1.7601.18762
Vulnerable range: Version Less than - 6.1.7601.18952
```

Impact
Successful exploitation will allow an attacker to conduct denial-of-service conditions and execute arbitrary code in the context of the currently logged-in user.
Impact Level: System

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-109

Affected Software/OS
Microsoft Windows Server 2012 Microsoft Windows Server 2012R2 Microsoft Windows 8/8.1 x32/x64 Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior.

Vulnerability Insight
Multiple flaws are due to: - Windows Shell fails to properly handle objects in memory. - Tablet Input Band fails to properly handle objects in memory.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`MS Windows Shell and Tablet Input Band Remote Code Execution Vulnerabilities (3.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.806090
Version used: `$Revision: 1938 $`

References
```
CVE: CVE-2015-2515, CVE-2015-2548
Other:
  URL:https://support.microsoft.com/en-us/kb/3096443
   URL:https://technet.microsoft.com/library/security/MS15-109
```

High (CVSS: 9.3)
NVT: Microsoft Office Suite Remote Code Execution Vulnerabilities (3089664)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-099.

Vulnerability Detection Result
```
File checked:     C:\Program Files\Common Files\Microsoft Shared\TextConvWpft532
↪.cnv
```

... continues on next page ...

... continued from previous page ...

```
File version:     2012.1500.4420.1017
Vulnerable range: 2012 - 2012.1500.4727.0009
```

Impact
Successful exploitation will allow a context-dependent attacker to corrupt memory and potentially execute arbitrary code.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-099

Affected Software/OS
Microsoft Office 2007 Service Pack 3 and prior Microsoft Office 2010 Service Pack 2 and prior Microsoft Office 2013 Service Pack 1 and prior.

Vulnerability Insight
A remote code execution exists in Microsoft Office that could be exploited when a user opens a file containing a malformed graphics image or when a user inserts a malformed graphics image into an Office file.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Suite Remote Code Execution Vulnerabilities (3089664)`
OID:1.3.6.1.4.1.25623.1.0.806109
Version used: `$Revision: 1689 $`

References
```
CVE: CVE-2015-2545
Other:
  URL:https://support.microsoft.com/en-us/kb/3089664
   URL:https://technet.microsoft.com/library/security/MS15-099
```

High (CVSS: 9.3)
NVT: Microsoft Office Excel Multiple Remote Code Execution Vulnerabilities (3089664)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-099.

Vulnerability Detection Result
```
File checked:  Excel.exe
File version:     15.0.4420.1017
Vulnerable range: 15 - 15.0.4753.0999
```

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms15-099

Affected Software/OS
Microsoft Excel 2007 Service Pack 3 and prior, Microsoft Excel 2010 Service Pack 2 and prior, Microsoft Excel 2013 Service Pack 1 and prior.

Vulnerability Insight
Multiple flaws exists when, - Microsoft Excel improperly handles the loading of dynamic link library (DLL) files. - Error when memory is released in an unintended manner. - Improper handling of files in the memory.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Excel Multiple Remote Code Execution Vulnerabilities (3089664)`
OID:1.3.6.1.4.1.25623.1.0.806110
Version used: `$Revision: 1689 $`

References
```
CVE: CVE-2015-2520, CVE-2015-2521, CVE-2015-2523
Other:
  URL:https://support.microsoft.com/en-us/kb/3089664
   URL:https://technet.microsoft.com/en-us/library/security/MS15-099
```

High (CVSS: 9.3)
NVT: Microsoft Office Excel Multiple Remote Code Execution Vulnerabilities (3096440)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS15-110.

Vulnerability Detection Result
```
File checked:  Excel.exe
File version:     15.0.4420.1017
Vulnerable range: 15 - 15.0.4763.0999
```

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.
Impact Level: System/Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms15-110

Affected Software/OS
Microsoft Excel 2007 Service Pack 3 and prior, Microsoft Excel 2010 Service Pack 2 and prior, Microsoft Excel 2013 Service Pack 1 and prior.

Vulnerability Insight
Multiple flaws exists when, - Microsoft Excel improperly handles the loading of dynamic link library (DLL) files. - Error when memory is released in an unintended manner. - Improper handling of files in the memory.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Excel Multiple Remote Code Execution Vulnerabilities (3096440)`
OID:1.3.6.1.4.1.25623.1.0.806120
Version used: `$Revision: 1938 $`

References
```
CVE: CVE-2015-2555, CVE-2015-2557, CVE-2015-2558
Other:
  URL:https://support.microsoft.com/en-us/kb/3096440
   URL:https://support.microsoft.com/en-us/kb/3085615
   URL:https://support.microsoft.com/en-us/kb/3085609
   URL:https://support.microsoft.com/en-us/kb/3085583
   URL:https://technet.microsoft.com/en-us/library/security/MS15-110
```

High (CVSS: 9.3)
NVT: Microsoft Office Access Database Remote Code Execution Vulnerabilities (2848637)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-074.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute the arbitrary code via a specially crafted ACCDB file and compromise the system.
Impact Level: System/Application

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms13-074

Affected Software/OS
Microsoft Office 2013 Microsoft Office 2007 Service Pack 3 and prior Microsoft Office 2010 Service Pack 2 and prior

Vulnerability Insight
Multiple flaws are due to errors when processing ACCDB files.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Access Database Remote Code Execution Vulnerabilities (2848637)`
OID:1.3.6.1.4.1.25623.1.0.902995
Version used: `$Revision: 1559 $`

References
```
CVE: CVE-2013-3155, CVE-2013-3156, CVE-2013-3157
BID:62229, 62230, 62231
Other:
  URL:http://secunia.com/advisories/51856
   URL:http://support.microsoft.com/kb/2687423
   URL:http://support.microsoft.com/kb/2687425
   URL:http://support.microsoft.com/kb/2810009
   URL:https://technet.microsoft.com/en-us/security/bulletin/ms13-074
```

High (CVSS: 9.3)
NVT: Microsoft Office Excel Remote Code Execution Vulnerabilities (2858300)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-073.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to corrupt memory and disclose sensitive information.
Impact Level: Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms13-073

Affected Software/OS
Microsoft Excel 2013 Microsoft Excel 2003 Service Pack 3 and prior Microsoft Excel 2007 Service Pack 3 and prior Microsoft Excel 2010 Service Pack 2 and prior

Vulnerability Insight
Multiple flaws exists when processing XML data, which can be exploited to disclose contents of certain local files by sending specially crafted XML data including external entity references.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Excel Remote Code Execution Vulnerabilities (2858300)`
OID:1.3.6.1.4.1.25623.1.0.902997
Version used: `$Revision: 1559 $`

References
```
CVE: CVE-2013-1315, CVE-2013-3158, CVE-2013-3159
BID:62167, 62219, 62225
Other:
  URL:http://support.microsoft.com/kb/2810048
   URL:http://support.microsoft.com/kb/2760583
   URL:http://support.microsoft.com/kb/2760597
   URL:http://support.microsoft.com/kb/2768017
   URL:http://technet.microsoft.com/en-us/security/bulletin/ms13-073
```

High (CVSS: 9.3)
NVT: Microsoft Office Remote Code Execution Vulnerabilities (2885080)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-085.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute the arbitrary code, cause memory corruption and compromise the system.
Impact Level: System/Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms13-085

Affected Software/OS
Microsoft Office 2013 Microsoft Office 2007 Service Pack 3 and prior Microsoft Office 2010 Service Pack 2 and prior

Vulnerability Insight
Multiple flaws are due to error when processing Microsoft Word binary documents can be exploited to cause a memory corruption

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Remote Code Execution Vulnerabilities (2885080)`
OID:1.3.6.1.4.1.25623.1.0.903407
Version used: `$Revision: 1559 $`

References
`CVE: CVE-2013-3889, CVE-2013-3890`
`BID:62829, 62824`
`Other:`
`URL:http://secunia.com/advisories/55141`
`URL:http://support.microsoft.com/kb/2760585`
`URL:http://support.microsoft.com/kb/2760591`
`URL:http://support.microsoft.com/kb/2826023`
`URL:http://support.microsoft.com/kb/2826035`
`URL:http://support.microsoft.com/kb/2817623`
`URL:https://technet.microsoft.com/en-us/security/bulletin/ms13-085`

High (CVSS: 9.3)
NVT: Microsoft Office Excel Remote Code Execution Vulnerabilities (2885080)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-085.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute the arbitrary code, cause memory corruption and compromise the system.
Impact Level: System/Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms13-085

Affected Software/OS
Microsoft Excel 2013 Microsoft Excel 2007 Service Pack 3 and prior Microsoft Excel 2010 Service Pack 2 and prior

Vulnerability Insight
Multiple flaws are due to error when processing Microsoft Word binary documents can be exploited to cause a memory corruption

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Excel Remote Code Execution Vulnerabilities (2885080)`
OID:1.3.6.1.4.1.25623.1.0.903408
Version used: `$Revision: 1559 $`

References
```
CVE: CVE-2013-3889, CVE-2013-3890
BID:62829, 62824
Other:
  URL:http://secunia.com/advisories/55141
   URL:http://support.microsoft.com/kb/2827324
   URL:http://support.microsoft.com/kb/2826033
   URL:http://support.microsoft.com/kb/2827238
   URL:https://technet.microsoft.com/en-us/security/bulletin/ms13-085
```

High (CVSS: 9.3)
NVT: Microsoft Office Remote Code Execution Vulnerabilities (2885093)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-091.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to corrupt memory, cause a buffer overflow and execution the arbitrary code.
Impact Level: System/Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms13-091

Affected Software/OS
Microsoft Office 2013 Microsoft Office 2003 Service Pack 3 and prior Microsoft Office 2007 Service Pack 3 and prior Microsoft Office 2010 Service Pack 1 and prior

Vulnerability Insight
Flaws are due to an error when parsing WordPerfect documents files (.wpd).

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Remote Code Execution Vulnerabilities (2885093)`
OID:1.3.6.1.4.1.25623.1.0.903414
Version used: `$Revision: 1559 $`

References
`CVE: CVE-2013-0082, CVE-2013-1324, CVE-2013-1325`
`BID:63559, 63569, 63570`
`Other:`
`URL:http://secunia.com/advisories/55539`
`URL:http://support.microsoft.com/kb/2760494`
`URL:http://support.microsoft.com/kb/2760781`
`URL:http://support.microsoft.com/kb/2768005`
`URL:http://technet.microsoft.com/en-us/security/bulletin/ms13-091`

High (CVSS: 9.3)
NVT: Microsoft Office Word Remote Code Execution Vulnerabilities (2916605)

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-001.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute the arbitrary code, cause memory corruption and compromise the system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms14-001

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Microsoft Word 2013 Microsoft Word 2003 Service Pack 3 and prior Microsoft Word 2007 Service Pack 3 and prior Microsoft Word 2010 Service Pack 2 and prior.

Vulnerability Insight
Multiple flaws are due to error exists when processing specially crafted office file.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Word Remote Code Execution Vulnerabilities (2916605)`
OID:1.3.6.1.4.1.25623.1.0.903426
Version used: `$Revision: 1559 $`

References
```
CVE: CVE-2014-0258, CVE-2014-0259, CVE-2014-0260
BID:64726, 64727, 64728
Other:
  URL:https://support.microsoft.com/kb/2863866
   URL:https://support.microsoft.com/kb/2837617
   URL:https://support.microsoft.com/kb/2863902
   URL:https://support.microsoft.com/kb/2863901
   URL:https://support.microsoft.com/kb/2827224
   URL:https://support.microsoft.com/kb/2863834
   URL:http://technet.microsoft.com/en-us/security/bulletin/ms14-001
```

High (CVSS: 8.3)
NVT: Microsoft Group Policy Remote Code Execution Vulnerability (3000483)

Summary
This host is missing an critical security update according to Microsoft Bulletin MS15-011.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow context-dependent to execute arbitrary code. Failed exploit attempts will result in a denial-of-service condition.
Impact Level: System

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-011

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Microsoft Windows 2003 x32/x64 Edition Service Pack 2 Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior Microsoft Windows Server 2008 x32 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x64 Edition Service Pack 2 Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows 8 x32/x64 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012/2012R2

Vulnerability Insight
The flaw is due to remote code execution vulnerability in the way Group Policy receives and applies policy data if a domain-joined system is connected to a domain controller

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Group Policy Remote Code Execution Vulnerability (3000483)`
OID:1.3.6.1.4.1.25623.1.0.805448
Version used: `$Revision: 1239 $`

References
`CVE: CVE-2015-0008`
`BID:72477`
`Other:`
`URL:http://osvdb.org/118181`
`URL:https://support.microsoft.com/kb/3000483`
`URL:https://technet.microsoft.com/library/security/ms15-011`

High (CVSS: 7.5)
NVT: Google Chrome Multiple Vulnerabilities-01 Oct15 (Windows)

Summary
The host is installed with Google Chrome and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 44.0.2403.157`
`Fixed version: 46.0.2490.71`

Impact
Successful exploitation would allow an attacker to cause a denial of service or possibly have other impact, bypass the security restrictions and gain access to potentially sensitive information.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Google Chrome version 46.0.2490.71 or later, For updates refer to http://www.google.com/chrome

Affected Software/OS
Google Chrome versions prior to 46.0.2490.71 on Windows.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Google Chrome Multiple Vulnerabilities-01 Oct15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805994
Version used: `$Revision: 1980 $`

References
```
CVE: CVE-2015-7834, CVE-2015-6763, CVE-2015-6762, CVE-2015-6761, CVE-2015-6760,
↪CVE-2015-6759, CVE-2015-6758, CVE-2015-6757, CVE-2015-6756, CVE-2015-6755
Other:
  URL:http://googlechromereleases.blogspot.in/2015/10/stable-channel-update.html
```

High (CVSS: 7.5)
NVT: Google Chrome Multiple Vulnerabilities-02 Oct15 (Windows)

Summary
The host is installed with Google Chrome and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 44.0.2403.157
Fixed version:     45.0.2454.101
```

Impact
Successful exploitation would allow an attacker to bypass certain security restrictions.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Google Chrome version 45.0.2454.101 or later, For updates refer to http://www.google.com/chrome

Affected Software/OS
Google Chrome versions prior to 45.0.2454.101 on Windows.

Vulnerability Insight
Multiple flaws exists due to, - An error in 'object-observe.js' script in Google V8 which does not properly restrict method calls on access-checked objects. - An error in bindings/core/v8/V8DOMWrapper.h script in Blink which does not perform a rethrow action to propagate information about a cross-context exception.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

... continues on next page ...

... continued from previous page ...

Details:Google Chrome Multiple Vulnerabilities-02 Oct15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805997
Version used: $Revision: 1980 $

References
CVE: CVE-2015-1304, CVE-2015-1303
Other:
URL:http://googlechromereleases.blogspot.in/2015/09/stable-channel-update_24.html

High (CVSS: 7.5)
NVT: Google Chrome Multiple Vulnerabilities-01 September15 (Windows)

Summary
The host is installed with Google Chrome and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 44.0.2403.157
Fixed version: 45.0.2454.85

Impact
Successful exploitation will allow remote attackers to bypass security restrictions, cause a denial of service condition or potentially execute arbitrary code, conduct spoofing attack, gain sensitive information, trigger specific actions and other unspecified impacts.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Google Chrome version 45.0.2454.85 or later, For updates refer to http://www.google.com/chrome

Affected Software/OS
Google Chrome version prior to 45.0.2454.85 on Windows.

Vulnerability Insight
Multiple flaws are due to: - Use-after-free vulnerability in the shared-timer implementation in Blink. - Double free vulnerability in OpenJPEG before r3002, as used in PDFium. - Multiple vulnerabilities in Blink. - Improper validation of user supplied input for setUninstallURL preference. - Improper handling of requests by WebRequest API implementation. - Error in UnescapeURLWithAdjustmentsImpl implementation. - Multiple use-after-free vulnerabilities in the PrintWebViewHelper class. - Use-after-free vulnerability in the 'SkMatrix::invertNonIdentity' function in core/SkMatrix.cpp script in Skia. - Multiple unspecified vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Google Chrome Multiple Vulnerabilities-01 September15 (Windows)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.806039
Version used: $Revision: 1699 $

References
CVE: CVE-2015-6583, CVE-2015-6582, CVE-2015-6581, CVE-2015-6580, CVE-2015-1301, ↪CVE-2015-1300, CVE-2015-1299, CVE-2015-1298, CVE-2015-1297, CVE-2015-1296, CVE ↪-2015-1295, CVE-2015-1294, CVE-2015-1293, CVE-2015-1292, CVE-2015-1291
Other:
URL:http://googlechromereleases.blogspot.in/2015/09/stable-channel-update.html

High (CVSS: 7.2)
NVT: Microsoft Windows Graphics Component Privilege Elevation Vulnerability (3069392)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-072.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain elevated priveleges.
Impact Level: System

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/library/security/MS15-072

Affected Software/OS
Microsoft Windows 8 x32/x64 Microsoft Windows 8.1 x32/x64 Microsoft Windows Server 2012 Microsoft Windows Server 2012 R2 Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows 2003 x32/x64 Edition Service Pack 2 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight
Flaw exists due to error when windows graphics component fails to properly process bitmap conversions.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:Microsoft Windows Graphics Component Privilege Elevation Vulnerability (3069392)
OID:1.3.6.1.4.1.25623.1.0.805920
Version used: $Revision: 1488 $

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2015-2364
Other:
URL:https://support.microsoft.com/en-us/kb/3069392
URL:https://technet.microsoft.com/en-us/library/security/MS15-072

High (CVSS: 7.2)
NVT: MS Windows Task Management Privilege Elevation Vulnerabilities (3089657)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-102.

Vulnerability Detection Result
File checked: C:\Windows\system32\Schedsvc.dll
File version: 6.1.7601.17514
Vulnerable range: Version Less than 6.1.7601.18951

Impact
Successful exploitation will allow attacker to gain elevated privileges to perform arbitrary administration functions such as add users and install applications on the targeted machine.
Impact Level: System

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-102

Affected Software/OS
Microsoft Windows 8 x32/x64 Microsoft Windows 8.1 x32/x64 Microsoft Windows 10 x32/x64 Microsoft Windows Server 2012 Microsoft Windows Server 2012R2 Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior.

Vulnerability Insight
Multiple flaws are due to, - Task Management failing to validate and enforce impersonation levels. - Task Scheduler failing to properly verify certain file system interactions.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:MS Windows Task Management Privilege Elevation Vulnerabilities (3089657)
OID:1.3.6.1.4.1.25623.1.0.806045
Version used: $Revision: 1729 $

References
CVE: CVE-2015-2524, CVE-2015-2525, CVE-2015-2528

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:https://support.microsoft.com/en-us/kb/3082089
   URL:https://support.microsoft.com/en-us/kb/3084135
   URL:https://technet.microsoft.com/library/security/MS15-102
```

[return to 192.168.1.25]

2.1.2 Medium general/tcp

Medium (CVSS: 6.9)
NVT: MS Windows HID Functionality(Over USB) Code Execution Vulnerability

Summary
This host is installed with USB device driver software and is prone to code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allows user-assisted attackers to execute arbitrary programs via crafted USB data.
Impact Level: System/Application

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
Micorsoft Windows 7 Microsoft Windows XP Service Pack 2 and prior Microsoft Windows 2k Service Pack 4 and prior Microsoft Windows 2K3 Service Pack 2 and prior Microsoft Windows 2k8 Service Pack 4 and prior Microsoft Windows Vista service Pack 2 and prior

Vulnerability Insight
The flaw is due to error in USB divice driver, which does not properly warn the user before enabling additional Human Interface Device (HID) functionality.

Vulnerability Detection Method
Details:`MS Windows HID Functionality(Over USB) Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801581
Version used: `$Revision: 1642 $`

References
`CVE: CVE-2011-0638`
`Other:`

... continues on next page ...

... continued from previous page ...

URL:http://www.cs.gmu.edu/~astavrou/publications.html
URL:http://news.cnet.com/8301-27080_3-20028919-245.html
URL:http://www.blackhat.com/html/bh-dc-11/bh-dc-11-briefings.html#Stavrou

Medium (CVSS: 6.9)
NVT: MS Malicious Software Removal Tool Privilege Escalation Security Advisory (3057154)

Summary
This host is missing an important security update according to Microsoft advisory 3057154.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to gain elevated privileges on the affected machine.
Impact Level: System

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/3074162

Affected Software/OS
Microsoft Malicious Software Removal Tool versions prior to 5.26.11603.0

Vulnerability Insight
The error exists as Microsoft Malicious Software Removal Tool (MSRT) fails to properly handle a race condition involving a DLL-planting scenario.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:MS Malicious Software Removal Tool Privilege Escalation Security Advisory (3057.
↪..
OID:1.3.6.1.4.1.25623.1.0.805937
Version used: $Revision: 1498 $

References
CVE: CVE-2015-2418
BID:75962
Other:
URL:https://technet.microsoft.com/library/security/3074162

Medium (CVSS: 6.8)
NVT: VLC Media Player Multiple Vulnerabilities Jan15 (Windows)

... continues on next page ...

... continued from previous page ...

Summary
The host is installed with VLC Media player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 2.1.5
Fixed version:     2.2.0-rc2
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to VideoLAN VLC media player version 2.2.0-rc2 or later. For updates refer to http://www.videolan.org/vlc

Affected Software/OS
VideoLAN VLC media player 2.1.5 on Windows.

Vulnerability Insight

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`VLC Media Player Multiple Vulnerabilities Jan15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805425
Version used: `$Revision: 1812 $`

References
```
CVE: CVE-2014-9598, CVE-2014-9597
BID:72106, 72105
Other:
  URL:http://osvdb.org/116451
   URL:http://osvdb.org/117450
   URL:http://seclists.org/fulldisclosure/2015/Jan/72
   URL:http://packetstormsecurity.com/files/130004
```

Medium (CVSS: 6.8)
NVT: Google Chrome Denial of Service Vulnerability September15 (Windows)

Summary
The host is installed with Google Chrome and is prone to denial of service vulnerability.

Vulnerability Detection Result
```
Installed version: 44.0.2403.157
```

... continues on next page ...

... continued from previous page ...

Fixed version: NoneAvailable

Impact
Successful exploitation could allow attackers to crash the application.
Impact Level: Application

Solution
Solution type: NoneAvailable
No solution or patch is available as of 20th September, 2015. Information regarding this issue will be updated once the solution details are available, For updates refer to http://www.google.com/chrome

Affected Software/OS
Google Chrome version 45.0.2454.93 and prior on Windows.

Vulnerability Insight
The flaw is due to browser address field does not properly sanitize user supplied input.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Google Chrome Denial of Service Vulnerability September15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.806054
Version used: $Revision: 1784 $

References
Other:
URL:http://www.dnaindia.com/scitech/report-a-vulnerability-in-google-chrome-ca
↪uses-it-to-crash-by-entering-a-simple-text-string-2127143

Medium (CVSS: 6.8)
NVT: VLC Media Player 3GP File Denial of Service Vulnerability Oct15 (Windows)

Summary
The host is installed with VLC media player and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 2.1.5
Fixed version: Not Available

Impact
Successful exploitation will allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted 3GP file.
Impact Level: System/Application

Solution
Solution type: NoneAvailable

... continues on next page ...

... continued from previous page ...

No solution or update is available as of 16th October, 2015. Information regarding this issue will be updated once the solution details are available. For updates refer to http://www.videolan.org

Affected Software/OS
VideoLAN VLC media player 2.2.1 and earlier on Windows.

Vulnerability Insight
The flaw is due to insufficient restrictions on a writable buffer which affects the 3GP file format parser.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`VLC Media Player 3GP File Denial of Service Vulnerability Oct15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.806086
Version used: `$Revision: 1961 $`

References
`CVE: CVE-2015-5949`
`BID:76448`
`Other:`
`URL:https://packetstormsecurity.com/files/133266`
`URL:http://www.securityfocus.com/archive/1/archive/1/536287/100/0/threaded`

Medium (CVSS: 5.0)
NVT: Microsoft Outlook Information Disclosure Vulnerability (2894514)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-094.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to disclose certain sensitive information.
Impact Level: Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms13-094

Affected Software/OS
Microsoft Outlook 2013 Microsoft Outlook 2007 Service Pack 3 and prior Microsoft Outlook 2010 Service Pack 2 and prior

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw is due to an error during the expansion of the S/MIME certificate metadata when validating the X.509 certificate chain and can be exploited to gain knowledge IP addresses and open TCP ports from the host and the connected LAN via a specially crafted S/MIME certificate sent in an email.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Outlook Information Disclosure Vulnerability (2894514)`
OID:1.3.6.1.4.1.25623.1.0.903413
Version used: `$Revision: 1559 $`

References
`CVE: CVE-2013-3905`
`BID:63603`
`Other:`
`URL:http://www.osvdb.org/99653`
`URL:http://secunia.com/advisories/55574`
`URL:http://securitytracker.com/id/1029328`
`URL:http://support.microsoft.com/kb/2825644`
`URL:http://support.microsoft.com/kb/2837597`
`URL:http://support.microsoft.com/kb/2837618`
`URL:http://technet.microsoft.com/en-us/security/bulletin/ms13-094`

Medium (CVSS: 4.3)
NVT: Microsoft Office Excel Multiple Remote Code Execution Vulnerabilities (3080790)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-081.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms15-081

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Microsoft Excel 2007 Service Pack 3 and prior, Microsoft Excel 2010 Service Pack 2 and prior, Microsoft Excel 2013 Service Pack 1 and prior.

Vulnerability Insight
Multiple flaws exists when, - Microsoft Excel improperly handles the loading of dynamic link library (DLL) files. - Error when memory is released in an unintended manner. - Improper handling of files in the memory.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office Excel Multiple Remote Code Execution Vulnerabilities (3080790)`
OID:1.3.6.1.4.1.25623.1.0.805088
Version used: `$Revision: 1695 $`

References
`CVE: CVE-2015-2423`
`Other:`
`URL:https://support.microsoft.com/en-us/kb/3054992`
`URL:https://support.microsoft.com/en-us/kb/3055044`
`URL:https://support.microsoft.com/en-us/kb/3054991`
`URL:https://technet.microsoft.com/en-us/library/security/MS15-081`

Medium (CVSS: 4.3)
NVT: Microsoft Office PowerPoint Multiple Remote Code Execution Vulnerabilities (3080790)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-081.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.
Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms15-081

Affected Software/OS
Microsoft PowerPoint 2007 Service Pack 3 and prior, Microsoft PowerPoint 2010 Service Pack 2 and prior, Microsoft PowerPoint 2013 Service Pack 1 and prior.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Flaws are due to improper handling of files in the memory.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft Office PowerPoint Multiple Remote Code Execution Vulnerabilities (308.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.805089
Version used: `$Revision: 1653 $`

References
`CVE: CVE-2015-2423`
`Other:`
`URL:https://support.microsoft.com/en-us/kb/3055051`
`URL:https://support.microsoft.com/en-us/kb/3055033`
`URL:https://support.microsoft.com/en-us/kb/3055029`
`URL:https://technet.microsoft.com/en-us/library/security/MS15-081`

Medium (CVSS: 4.3)
NVT: Microsoft DES Encryption Security Advisory (3057154)

Summary
This host is missing an important security update according to Microsoft advisory (3057154).

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to break certain authentication scenarios.
Impact Level: System

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/3057154

Affected Software/OS
Microsoft Windows 8 x32/x64 Microsoft Windows Server 2012 Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior.

Vulnerability Insight
An update is available that provides enhanced user protection in environments where DES is still enabled for application compatibility reasons.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`Microsoft DES Encryption Security Advisory (3057154)`
OID:1.3.6.1.4.1.25623.1.0.805678
Version used: `$Revision: 1491 $`

References
```
Other:
  URL:https://support.microsoft.com/en-us/kb/3057154
   URL:https://technet.microsoft.com/library/security/3057154
```

Medium (CVSS: 4.3)
NVT: MS Windows XML Core Services Information Disclosure Vulnerability (3080129)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-084.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to conduct man-in-the-middle (MiTM) attack and gain access to sensitive data.
Impact Level: System

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/ms15-084

Affected Software/OS
Microsoft Windows 8 x32/x64 Microsoft Windows Server 2012 Microsoft Windows 8.1 x32/x64 Microsoft Windows Server 2012 R2 Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Vulnerability Insight
Flaw exists due to, - An error in Microsoft XML Core Services which allows forceful use of Secure Sockets Layer (SSL) 2.0. - An error in Microsoft XML Core Services which exposes memory addresses not intended for public disclosure.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:`MS Windows XML Core Services Information Disclosure Vulnerability (3080129)`
OID:1.3.6.1.4.1.25623.1.0.805950
Version used: `$Revision: 1563 $`

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2015-2434, CVE-2015-2471, CVE-2015-2440
BID:76232, 76257, 76229
Other:
URL:https://support.microsoft.com/en-us/kb/3076895
URL:https://support.microsoft.com/en-us/kb/3080129
URL:https://technet.microsoft.com/library/security/ms15-084

Medium (CVSS: 4.3)
NVT: MS Windows Command Line Parameter Information Disclosure Vulnerability (3082458)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-088.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow a local attacker to obtain sensitive information that may aid in further attacks.
Impact Level: System

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-088

Affected Software/OS
Microsoft Windows 8 x32/x64 Microsoft Windows 8.1 x32/x64 Microsoft Windows 10 x32/x64 Microsoft Windows Server 2012 Microsoft Windows Server 2012R2 Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior.

Vulnerability Insight
The flaw is due to an improper security restrictions on files stored on an affected system.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:MS Windows Command Line Parameter Information Disclosure Vulnerability (3082458)
OID:1.3.6.1.4.1.25623.1.0.806012
Version used: $Revision: 1695 $

References
CVE: CVE-2015-2423

... continues on next page ...

... continued from previous page ...

BID:76202
Other:
URL:https://support.microsoft.com/en-us/kb/3046017
URL:https://support.microsoft.com/en-us/kb/3079757
URL:https://technet.microsoft.com/library/security/MS15-088

Medium (CVSS: 4.3)
NVT: Microsoft Office Information Disclosure Vulnerability (2909976)

Summary
This host is missing an important security update according to Microsoft Bulletin MS13-104.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to disclose certain sensitive information.
Impact Level: Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/en-us/security/bulletin/ms13-104

Affected Software/OS
Microsoft Office 2013

Vulnerability Insight
The flaw is due to the application improperly handling response while attempting to open a hosted file and can be exploited to disclose tokens used to authenticate the user on a SharePoint or other Microsoft Office server site.

Vulnerability Detection Method
Get the vulnerable file version and check appropriate patch is applied or not.
Details:Microsoft Office Information Disclosure Vulnerability (2909976)
OID:1.3.6.1.4.1.25623.1.0.903419
Version used: $Revision: 1559 $

References
CVE: CVE-2013-5054
BID:64092
Other:
URL:http://secunia.com/advisories/55997
URL:http://support.microsoft.com/kb/2850064
URL:http://www.securitytracker.com/id/1029464
URL:https://technet.microsoft.com/en-us/security/bulletin/ms13-104

[return to 192.168.1.25]

2.1.3 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE Services Enumeration

Summary
Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.
An attacker may use this fact to gain more knowledge about the remote host.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
filter incoming traffic to this port.

Vulnerability Detection Method
Details:`DCE Services Enumeration`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `$Revision: 41 $`

Medium (CVSS: 5.0)
NVT: DCE Services Enumeration

Summary
Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.
An attacker may use this fact to gain more knowledge about the remote host.

Vulnerability Detection Result

```
Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.
An attacker may use this fact to gain more knowledge
about the remote host.
Here is the list of DCE services running on this host:
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.25[49152]
Port: 49153/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.25[49153]
     Annotation: Event log TCPIP
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.25[49153]
```

...continues on next page ...

. . . continued from previous page . . .

```
      Annotation: NRP server endpoint
      UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.25[49153]
      Annotation: DHCPv6 Client LRPC Endpoint
      UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.25[49153]
      Annotation: DHCP Client LRPC Endpoint
      UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.25[49153]
      Annotation: Security Center
Port: 49154/tcp
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.25[49154]
      UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.25[49154]
      Annotation: IP Transition Configuration endpoint
      UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.25[49154]
      Annotation: XactSrv service
Port: 49155/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.1.25[49155]
Port: 49156/tcp
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.25[49156]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
Solution : filter incoming traffic to this port(s).
```

Solution
filter incoming traffic to this port.

Vulnerability Detection Method
Details:`DCE Services Enumeration`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `$Revision: 41 $`

[return to 192.168.1.25]

2.1.4 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary

. . . continues on next page . . .

... continued from previous page ...

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Paket 1: 614784
Paket 2: 614891
```

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS

TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details:`TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 787 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
```

[return to 192.168.1.25]

2.1.5 Log general/tcp

Log (CVSS: 0.0)
NVT: OS fingerprinting

Summary

... continues on next page ...

... continued from previous page ...

This script performs ICMP based OS fingerprinting (as described by Ofir Arkin and Fyodor Yarochkin in Phrack 57). It can be used to determine remote operating system version.

Vulnerability Detection Result

```
ICMP based OS fingerprint results: (80% confidence)
HP JetDirect
```

Log Method

Details:`OS fingerprinting`
OID:1.3.6.1.4.1.25623.1.0.102002
Version used: `$Revision: 1739 $`

References

```
Other:
  URL:http://www.phrack.org/issues.html?issue=57&amp;id=7#article
```

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

```
DIRB could not be found in your system path.
OpenVAS was unable to execute DIRB and to perform the scan you
requested.
Please make sure that DIRB is installed and is
available in the PATH variable defined for your environment.
```

Log Method

Details:`DIRB (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: `$Revision: 13 $`

Log (CVSS: 0.0)
NVT: SMB Registry : Windows Service Pack version

Summary

Detection of installed Windows Service Pack version.
The script logs in via SMB, and reads the registry key to retrieve Windows Service Pack Version and sets KnowledgeBase.

Vulnerability Detection Result

```
The Windows 7 Ultimate 6.1 is installed with Service Pack 1
```

... continues on next page ...

... continued from previous page ...

Log Method
Details:`SMB Registry : Windows Service Pack version`
OID:1.3.6.1.4.1.25623.1.0.10401
Version used: `$Revision: 549 $`

Log (CVSS: 0.0)
NVT: arachni (NASL wrapper)

Summary
This plugin uses arachni ruby command line to find web security issues.
See the preferences section for arachni options.
Note that OpenVAS is using limited set of arachni options. Therefore, for more complete web assessment, you should use standalone arachni tool for deeper/customized checks.

Vulnerability Detection Result
```
Arachni could not be found in your system path.
OpenVAS was unable to execute Arachni and to perform the scan you
requested.
Please make sure that Arachni is installed and that arachni is
available in the PATH variable defined for your environment.
```

Log Method
Details:`arachni (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.110001
Version used: `$Revision: 683 $`

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result
```
Here is the route from 192.168.1.22 to 192.168.1.25:
192.168.1.22
192.168.1.25
```

Solution
Block unwanted packets from escaping your network.

Log Method
Details:`Traceroute`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 975 $

Log (CVSS: 0.0)
NVT: Google Chrome Version Detection (Windows)

Summary
Detection of installed version of Google Chrome on Windows.
The script logs in via smb, searches for Google Chrome in the registry and gets the version from registry.

Vulnerability Detection Result
```
Detected Google Chrome
Version: 44.0.2403.157
Location: C:\Program Files (x86)\Google\Chrome\Application
CPE: cpe:/a:google:chrome:44.0.2403.157
Concluded from version identification result:
44.0.2403.157
```

Log Method
Details:Google Chrome Version Detection (Windows)
OID:1.3.6.1.4.1.25623.1.0.800120
Version used: $Revision: 372 $

Log (CVSS: 0.0)
NVT: Microsoft Internet Explorer Version Detection (Win)

Summary
Detection of installed version of Microsoft Internet Explorer.
The script logs in via smb, detects the version of Microsoft Internet Explorer on remote host and sets the KB.

Vulnerability Detection Result
```
Detected Microsoft Internet Explorer
Version: 11.0.9600.17914
Location: C:\Program Files\Internet Explorer
CPE: cpe:/a:microsoft:ie:11.0.9600.17914
Concluded from version identification result:
11.0.9600.17914
```

Log Method
Details:Microsoft Internet Explorer Version Detection (Win)
OID:1.3.6.1.4.1.25623.1.0.800209
Version used: $Revision: 42 $

Log (CVSS: 0.0)
NVT: Sun Java Products Version Detection (Win)

Summary
Detection of installed version of Java Products.
The script logs in via smb, searches for Java Products in the registry and gets the version from 'Version' string in registry

Vulnerability Detection Result
```
Detected Oracle Java JDK
Version: 1.8.0_45
Location: C:\Program Files\Java\jdk1.8.0_45
CPE: cpe:/a:oracle:jdk:1.8.0:update_45
Concluded from version identification result:
1.8.0_45
```

Log Method
Details:`Sun Java Products Version Detection (Win)`
OID:1.3.6.1.4.1.25623.1.0.800383
Version used: `$Revision: 1934 $`

Log (CVSS: 0.0)
NVT: Sun Java Products Version Detection (Win)

Summary
Detection of installed version of Java Products.
The script logs in via smb, searches for Java Products in the registry and gets the version from 'Version' string in registry

Vulnerability Detection Result
```
Detected Oracle Java JDK
Version: 1.8.0_45
Location: C:\Program Files\Java\jdk1.8.0_45
CPE: cpe:/a:oracle:jdk:x64:1.8.0:update_45
Concluded from version identification result:
1.8.0_45
```

Log Method
Details:`Sun Java Products Version Detection (Win)`
OID:1.3.6.1.4.1.25623.1.0.800383
Version used: `$Revision: 1934 $`

Log (CVSS: 0.0)
NVT: Sun Java Products Version Detection (Win)

Summary

. . . continues on next page . . .

... continued from previous page ...

Detection of installed version of Java Products.
The script logs in via smb, searches for Java Products in the registry and gets the version from 'Version' string in registry

Vulnerability Detection Result

```
Detected Oracle Java JRE
Version: 1.8.0_45
Location: C:\Program Files\Java\jre1.8.0_45
CPE: cpe:/a:oracle:jre:1.8.0:update_45
Concluded from version identification result:
1.8.0_45
```

Log Method

Details:`Sun Java Products Version Detection (Win)`
OID:1.3.6.1.4.1.25623.1.0.800383
Version used: `$Revision: 1934 $`

Log (CVSS: 0.0)
NVT: Sun Java Products Version Detection (Win)

Summary

Detection of installed version of Java Products.
The script logs in via smb, searches for Java Products in the registry and gets the version from 'Version' string in registry

Vulnerability Detection Result

```
Detected Oracle Java JRE
Version: 1.8.0_45
Location: C:\Program Files\Java\jre1.8.0_45
CPE: cpe:/a:oracle:jre:x64:1.8.0:update_45
Concluded from version identification result:
1.8.0_45
```

Log Method

Details:`Sun Java Products Version Detection (Win)`
OID:1.3.6.1.4.1.25623.1.0.800383
Version used: `$Revision: 1934 $`

Log (CVSS: 0.0)
NVT: Microsoft SMB Signing Disabled

Summary

Checking for SMB signing is disabled.
The script logs in via smb, checks the SMB Negotiate Protocol response to confirm SMB signing is disabled.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
SMB signing is disabled on this host

Log Method
Details:Microsoft SMB Signing Disabled
OID:1.3.6.1.4.1.25623.1.0.802726
Version used: $Revision: 12 $

Log (CVSS: 0.0)
NVT: Microsoft OneNote Version Detection (Windows)

Summary
Detection of installed version of Microsoft OneNote.
The script logs in via smb, and detect the version of Microsoft OneNote on remote host and sets the KB

Vulnerability Detection Result
Detected Microsoft OneNote
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\Office15\
CPE: cpe:/a:microsoft:onenote:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017

Log Method
Details:Microsoft OneNote Version Detection (Windows)
OID:1.3.6.1.4.1.25623.1.0.803436
Version used: $Revision: 1128 $

Log (CVSS: 0.0)
NVT: Microsoft OneNote Version Detection (Windows)

Summary
Detection of installed version of Microsoft OneNote.
The script logs in via smb, and detect the version of Microsoft OneNote on remote host and sets the KB

Vulnerability Detection Result
Detected Microsoft OneNote
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\Office15\
CPE: cpe:/a:microsoft:onenote:x64:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017

... continues on next page ...

. . . continued from previous page . . .

Log Method
Details:`Microsoft OneNote Version Detection (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803436
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: Cygwin Version Detection (Windows)

Summary
Detection of installed version of Cygwin on Windows.
The script logs in via smb, searches for Cygwin in the registry and gets the version.

Vulnerability Detection Result
```
Detected Cygwin
Version: Unknown
Location: C:\cygwin64
CPE: cpe:/a:redhat:cygwin
Concluded from version identification result:
Unknown
```

Log Method
Details:`Cygwin Version Detection (Windows)`
OID:1.3.6.1.4.1.25623.1.0.806089
Version used: `$Revision: 1980 $`

Log (CVSS: 0.0)
NVT: Cygwin Version Detection (Windows)

Summary
Detection of installed version of Cygwin on Windows.
The script logs in via smb, searches for Cygwin in the registry and gets the version.

Vulnerability Detection Result
```
Detected Cygwin
Version: Unknown
Location: C:\cygwin64
CPE: cpe:/a:redhat:cygwin:x64
Concluded from version identification result:
Unknown
```

Log Method
Details:`Cygwin Version Detection (Windows)`
OID:1.3.6.1.4.1.25623.1.0.806089
Version used: `$Revision: 1980 $`

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary
Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

Vulnerability Detection Result
```
Detected Microsoft Office 32-bit Components 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\
CPE: cpe:/a:microsoft:office:2013:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017
```

Log Method
Details:`Microsoft Office Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900025
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary
Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

Vulnerability Detection Result
```
Detected Microsoft Office OSM MUI (French) 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\
CPE: cpe:/a:microsoft:office:2013:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017
```

Log Method
Details:`Microsoft Office Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900025
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary

. . . continues on next page . . .

... continued from previous page ...

Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

Vulnerability Detection Result

```
Detected Microsoft Office OSM MUI (French) 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\
CPE: cpe:/a:microsoft:office:2013:x64:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017
```

Log Method

Details:`Microsoft Office Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900025
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary

Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

Vulnerability Detection Result

```
Detected Microsoft Office OSM UX MUI (French) 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\
CPE: cpe:/a:microsoft:office:2013:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017
```

Log Method

Details:`Microsoft Office Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900025
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary

Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Detected Microsoft Office OSM UX MUI (French) 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\
CPE: cpe:/a:microsoft:office:2013:x64:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017

Log Method
Details:Microsoft Office Version Detection
OID:1.3.6.1.4.1.25623.1.0.900025
Version used: $Revision: 1128 $

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary
Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

Vulnerability Detection Result
Detected Microsoft Office Professional Plus 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\
CPE: cpe:/a:microsoft:office:2013:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017

Log Method
Details:Microsoft Office Version Detection
OID:1.3.6.1.4.1.25623.1.0.900025
Version used: $Revision: 1128 $

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary
Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

Vulnerability Detection Result
Detected Microsoft Office Professional Plus 2013

... continues on next page ...

... continued from previous page ...

```
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\
CPE: cpe:/a:microsoft:office:2013:x64:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017
```

Log Method
Details:Microsoft Office Version Detection
OID:1.3.6.1.4.1.25623.1.0.900025
Version used: $Revision: 1128 $

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary
Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

Vulnerability Detection Result

```
Detected Microsoft Office Professionnel Plus 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office
CPE: cpe:/a:microsoft:office:2013:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017
```

Log Method
Details:Microsoft Office Version Detection
OID:1.3.6.1.4.1.25623.1.0.900025
Version used: $Revision: 1128 $

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary
Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

Vulnerability Detection Result

```
Detected Microsoft Office Professionnel Plus 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office
CPE: cpe:/a:microsoft:office:2013:x64:15.0.4420.1017
```

... continues on next page ...

... continued from previous page ...

Concluded from version identification result:
15.0.4420.1017

Log Method
Details:Microsoft Office Version Detection
OID:1.3.6.1.4.1.25623.1.0.900025
Version used: $Revision: 1128 $

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary
Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

Vulnerability Detection Result
Detected Microsoft Office Proofing (French) 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\
CPE: cpe:/a:microsoft:office:2013:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017

Log Method
Details:Microsoft Office Version Detection
OID:1.3.6.1.4.1.25623.1.0.900025
Version used: $Revision: 1128 $

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary
Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

Vulnerability Detection Result
Detected Microsoft Office Proofing (French) 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\
CPE: cpe:/a:microsoft:office:2013:x64:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017

... continues on next page ...

. . . continued from previous page . . .

Log Method
Details:`Microsoft Office Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900025
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary
Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

Vulnerability Detection Result
```
Detected Microsoft Office Shared 32-bit MUI (French) 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\
CPE: cpe:/a:microsoft:office:2013:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017
```

Log Method
Details:`Microsoft Office Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900025
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary
Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

Vulnerability Detection Result
```
Detected Microsoft Office Shared MUI (French) 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\
CPE: cpe:/a:microsoft:office:2013:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017
```

Log Method
Details:`Microsoft Office Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900025

. . . continues on next page . . .

... continued from previous page ...

Version used: $Revision: 1128 $

Log (CVSS: 0.0)
NVT: Microsoft Office Version Detection

Summary
Detection of installed version of Microsoft Office.
The script logs in via smb, searches for Microsoft Office in the registry, gets version from the 'DisplayVersion' string and set it in the KB item.

Vulnerability Detection Result
```
Detected Microsoft Office Shared MUI (French) 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\
CPE: cpe:/a:microsoft:office:2013:x64:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017
```

Log Method
Details:Microsoft Office Version Detection
OID:1.3.6.1.4.1.25623.1.0.900025
Version used: $Revision: 1128 $

Log (CVSS: 0.0)
NVT: Microsoft Windows Media Player Version Detection

Summary
Detection of installed version of Windows Media Player.
The script logs in via smb, searches for Windows Media Player CLSID in the registry, gets version and set it in the KB item.

Vulnerability Detection Result
```
Detected Microsoft Windows Media Player
Version: 12.0.7601.18840
Location: ProgramFiles(x86)\Windows Media Player
CPE: cpe:/a:microsoft:windows_media_player:12.0.7601.18840
Concluded from version identification result:
12.0.7601.18840
```

Log Method
Details:Microsoft Windows Media Player Version Detection
OID:1.3.6.1.4.1.25623.1.0.900173
Version used: $Revision: 1128 $

Log (CVSS: 0.0)
NVT: VLC Media Player Version Detection (Win)

Summary
Detection of installed version of VLC Media Player version on Windows.
The script logs in via smb, searches for VLC Media Player in the registry and gets the version from registry.

Vulnerability Detection Result
```
Detected VLC Media Player
Version: 2.1.5
Location: C:\Program Files (x86)\VideoLAN\VLC
CPE: cpe:/a:videolan:vlc_media_player:2.1.5
Concluded from version identification result:
2.1.5
```

Log Method
Details:`VLC Media Player Version Detection (Win)`
OID:1.3.6.1.4.1.25623.1.0.900528
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: Microsoft Lync Version Detection

Summary
Detection of installed version of Microsoft Lync.
The script logs in via smb, searches for Microsoft Lync in the registry and gets the version from 'DisplayVersion' string in registry

Vulnerability Detection Result
```
Detected Microsoft Lync MUI (French) 2013
Version: 15.0.4420.1017
Location: C:\Program Files\Microsoft Office\
CPE: cpe:/a:microsoft:lync:2013::x64:15.0.4420.1017
Concluded from version identification result:
15.0.4420.1017
```

Log Method
Details:`Microsoft Lync Version Detection`
OID:1.3.6.1.4.1.25623.1.0.902843
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: Desktop Boards BIOS Information Detection for Windows

Summary

. . . continues on next page . . .

... continued from previous page ...

Detection of installed version of Desktop Boards BIOS.
The script logs in via smb and queries for the version.

Vulnerability Detection Result

```
Desktop Boards BIOS version V1.09 was detected on the host
Desktop Boards BIOS Vendor Phoenix Technologies LTD was detected on the host
Desktop Boards Base Board version V1.09 was detected on the host
Desktop Boards Base Board Manufacturer Packard Bell was detected on the host
Desktop Boards Base Board Product Name EasyNote LM86 was detected on the host
```

Log Method

Details:`Desktop Boards BIOS Information Detection for Windows`
OID:1.3.6.1.4.1.25623.1.0.96197
Version used: `$Revision: 1209 $`

[return to 192.168.1.25]

2.1.6 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary

This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.

Vulnerability Detection Result

```
192.168.1.25|cpe:/a:oracle:jdk:x64:1.8.0:update_45
192.168.1.25|cpe:/a:oracle:jdk:1.8.0:update_45
192.168.1.25|cpe:/a:oracle:jre:1.8.0:update_45
192.168.1.25|cpe:/a:oracle:jre:x64:1.8.0:update_45
192.168.1.25|cpe:/a:microsoft:onenote:15.0.4420.1017
192.168.1.25|cpe:/a:microsoft:onenote:x64:15.0.4420.1017
192.168.1.25|cpe:/a:microsoft:office_excel:2013
192.168.1.25|cpe:/a:microsoft:office_word:2013
192.168.1.25|cpe:/a:microsoft:office_publisher:2013
192.168.1.25|cpe:/a:microsoft:office_powerpoint:2013
192.168.1.25|cpe:/a:microsoft:access:2013
192.168.1.25|cpe:/a:microsoft:visio_viewer:2013
192.168.1.25|cpe:/a:microsoft:outlook:2013
192.168.1.25|cpe:/a:microsoft:ie:11.0.9600.17914
192.168.1.25|cpe:/a:redhat:cygwin
192.168.1.25|cpe:/a:redhat:cygwin:x64
192.168.1.25|cpe:/a:microsoft:lync:2013::x64:15.0.4420.1017
192.168.1.25|cpe:/a:microsoft:office:2013:x64:15.0.4420.1017
```

... continues on next page ...

... continued from previous page ...

```
192.168.1.25|cpe:/a:microsoft:office:2013:15.0.4420.1017
192.168.1.25|cpe:/a:videolan:vlc_media_player:2.1.5
192.168.1.25|cpe:/a:microsoft:windows_media_player:12.0.7601.18840
192.168.1.25|cpe:/a:google:chrome:44.0.2403.157
192.168.1.25|cpe:/o:microsoft:windows_7::sp1
```

Log Method
Details:`CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `$Revision: 314 $`

[return to 192.168.1.25]

2.1.7 Log 2869/tcp

Log (CVSS: 0.0)
NVT: Directories used for CGI Scanning

Summary
The script prints out the directories which are used when CGI scanning is enabled.

Vulnerability Detection Result

```
The following directories are used for CGI scanning:
/scripts
/cgi-bin
/
```

Log Method
Details:`Directories used for CGI Scanning`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `$Revision: 1727 $`

Log (CVSS: 0.0)
NVT: Identify unknown services with 'HELP'

Summary
This plugin performs service detection.
Description :

Vulnerability Detection Result

```
A (non-RFC compliant) web server seems to be running on this port
```

Log Method
Details:`Identify unknown services with 'HELP'`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.11153
Version used: $Revision: 1832 $

Log (CVSS: 0.0)
NVT: Hidden WWW server name

Summary
It seems that your web server tries to hide its version or name, which is a good thing. However, using a special crafted request, OpenVAS was able to discover it.

Vulnerability Detection Result

```
It seems that your web server tries to hide its version
or name, which is a good thing.
However, using a special crafted request, OpenVAS was able
to determine that is is running :
 Microsoft-HTTPAPI/2.0
Solution: Fix your configuration.
```

Solution
Fix your configuration.

Log Method
Details:Hidden WWW server name
OID:1.3.6.1.4.1.25623.1.0.11239
Version used: $Revision: 673 $

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

Summary
This plugin uses nikto(1) to find weak CGI scripts and other known issues regarding web server security. See the preferences section for configuration options.

Vulnerability Detection Result

```
Here is the Nikto report:
- Nikto v2.1.5
---------------------------------------------------------------------------
+ No web server found on blackyfox-1.home:2869
---------------------------------------------------------------------------
+ 0 host(s) tested
```

Log Method
Details:Nikto (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.14260
Version used: $Revision: 995 $

Log (CVSS: 0.0)
NVT: wapiti (NASL wrapper)

Summary
This plugin uses wapiti to find web security issues.
Make sure to have wapiti 2.x as wapiti 1.x is not supported.
See the preferences section for wapiti options.
Note that OpenVAS is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.

Vulnerability Detection Result
```
wapiti could not be found in your system path.
OpenVAS was unable to execute wapiti and to perform the scan you
requested.
Please make sure that wapiti is installed and that wapiti is
available in the PATH variable defined for your environment.
```

Log Method
Details:`wapiti (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.80110
Version used: `$Revision: 14 $`

[return to 192.168.1.25]

2.1.8 Log 139/tcp

Log (CVSS: 0.0)
NVT: SMB on port 445

Summary
This script detects wether port 445 and 139 are open and if thet are running SMB servers.

Vulnerability Detection Result
```
An SMB server is running on this port
```

Log Method
Details:`SMB on port 445`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `$Revision: 41 $`

[return to 192.168.1.25]

2.1.9 Log 445/tcp

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result
```
Summary:
 It is possible to extract OS, domain and SMB server information
from the Session Setup AndX Response packet which is generated
during NTLM authentication.Detected SMB workgroup: WORKGROUP
Detected SMB server: Windows 7 Ultimate 6.1
Detected OS: Windows 7 Ultimate 7601 Service Pack 1
```

Log Method
Details:`SMB NativeLanMan`
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: `$Revision: 43 $`

Log (CVSS: 0.0)
NVT: SMB Enumerate Services

Summary
This plugin implements the SvcOpenSCManager() and SvcEnumServices() calls to obtain the list of active and inactive services and drivers of the remote host, using the MS-DCE/RPC protocol over SMB.
An attacker may use this feature to gain better knowledge of the remote host.

Vulnerability Detection Result
```
WIN32 active services:
Expérience d[U+0092]application [AeLookupSvc]
AMD External Events Utility [AMD External Events Utility]
Générateur de points de terminaison du service Audio Windows [AudioEndpointBuild
↪er]
Audio Windows [AudioSrv]
Moteur de filtrage de base [BFE]
Service de transfert intelligent en arrière-plan [BITS]
Explorateur d[U+0092]ordinateurs [Browser]
Services de chiffrement [CryptSvc]
Fichiers hors connexion [CscService]
Lanceur de processus serveur DCOM [DcomLaunch]
Client DHCP [Dhcp]
Diagnostics Tracking Service [DiagTrack]
Client DNS [Dnscache]
Service de stratégie de diagnostic [DPS]
Protocole EAP (Extensible Authentication Protocol) [EapHost]
```

... continues on next page ...

... continued from previous page ...

```
Journal d[U+0092]événements Windows [eventlog]
Système d[U+0092]événement COM+ [EventSystem]
Hôte du fournisseur de découverte de fonctions [fdPHost]
Publication des ressources de découverte de fonctions [FDResPub]
Service de cache de police Windows [FontCache]
Client de stratégie de groupe [gpsvc]
Accès du périphérique d'interface utilisateur [hidserv]
Écouteur HomeGroup [HomeGroupListener]
Fournisseur HomeGroup [HomeGroupProvider]
Assistance IP [iphlpsvc]
Isolation de clé CNG [KeyIso]
Serveur [LanmanServer]
Station de travail [LanmanWorkstation]
Assistance NetBIOS sur TCP/IP [lmhosts]
Pare-feu Windows [MpsSvc]
Connexions réseau [Netman]
Service Liste des réseaux [netprofm]
Connaissance des emplacements réseau [NlaSvc]
Service Interface du magasin réseau [nsi]
Gestionnaire d[U+0092]identité réseau homologue [p2pimsvc]
Groupement de mise en réseau de pairs [p2psvc]
Service de l[U+0092]Assistant Compatibilité des programmes [PcaSvc]
Plug-and-Play [PlugPlay]
Protocole PNRP [PNRPsvc]
Alimentation [Power]
Service de profil utilisateur [ProfSvc]
Emplacement protégé [ProtectedStorage]
Registre à distance [RemoteRegistry]
Mappeur de point de terminaison RPC [RpcEptMapper]
Appel de procédure distante (RPC) [RpcSs]
Gestionnaire de comptes de sécurité [SamSs]
Planificateur de tâches [Schedule]
Service de notification d[U+0092]événements système [SENS]
Détection matériel noyau [ShellHWDetection]
Spouleur d[U+0092]impression [Spooler]
Découverte SSDP [SSDPSRV]
Acquisition d[U+0092]image Windows (WIA) [stisvc]
Thèmes [Themes]
Client de suivi de lien distribué [TrkWks]
Programme d[U+0092]installation pour les modules Windows [TrustedInstaller]
Hôte de périphérique UPnP [upnphost]
Gestionnaire de sessions du Gestionnaire de fenêtrage [UxSms]
Service hôte WDIServiceHost [WdiServiceHost]
Windows Defender [WinDefend]
Service de découverte automatique de Proxy Web pour les services HTTP Windows [W
↪inHttpAutoProxySvc]
Infrastructure de gestion Windows [Winmgmt]
```

... continues on next page ...

... continued from previous page ...

```
Service de configuration automatique WLAN [Wlansvc]
Service Partage réseau du Lecteur Windows Media [WMPNetworkSvc]
Centre de sécurité [wscsvc]
Windows Search [WSearch]
Windows Update [wuauserv]
##################################################
WIN32 inactive services:
Service de la passerelle de la couche Application [ALG]
Identité de l[U+0092]application [AppIDSvc]
Informations d[U+0092]application [Appinfo]
Gestion d[U+0092]applications [AppMgmt]
ASP.NET State Service [aspnet_state]
Programme d[U+0092]installation ActiveX (AxInstSV) [AxInstSV]
Service de chiffrement de lecteur BitLocker [BDESVC]
Service de prise en charge Bluetooth [bthserv]
Propagation du certificat [CertPropSvc]
Microsoft .NET Framework NGEN v2.0.50727_X86 [clr_optimization_v2.0.50727_32]
Microsoft .NET Framework NGEN v2.0.50727_X64 [clr_optimization_v2.0.50727_64]
Microsoft .NET Framework NGEN v4.0.30319_X86 [clr_optimization_v4.0.30319_32]
Microsoft .NET Framework NGEN v4.0.30319_X64 [clr_optimization_v4.0.30319_64]
Application système COM+ [COMSysApp]
Défragmenteur de disque [defragsvc]
Configuration automatique de réseau câblé [dot3svc]
Système de fichiers EFS (Encrypting File System) [EFS]
Service de réception Windows Media Center [ehRecvr]
Service de planification Windows Media Center [ehSched]
Télécopie [Fax]
Cache de police de Windows Presentation Foundation 3.0.0.0 [FontCache3.0.0.0]
Service Google Update (gupdate) [gupdate]
Service Google Update (gupdatem) [gupdatem]
Gestion des clés et des certificats d[U+0092]intégrité [hkmsvc]
Windows CardSpace [idsvc]
Internet Explorer ETW Collector Service [IEEtwCollectorService]
Modules de génération de clés IKE et AuthIP [IKEEXT]
Énumérateur de bus IP PnP-X [IPBusEnum]
Service KtmRm pour Distributed Transaction Coordinator [KtmRm]
Mappage de découverte de topologie de la couche de liaison [lltdsvc]
Service Media Center Extender [Mcx2Svc]
Planificateur de classes multimédias [MMCSS]
Coordinateur de transactions distribuées [MSDTC]
Service Initiateur iSCSI de Microsoft [MSiSCSI]
Windows Installer [msiserver]
Agent de protection d[U+0092]accès réseau [napagent]
Netlogon [Netlogon]
Net.Msmq Listener Adapter [NetMsmqActivator]
Net.Pipe Listener Adapter [NetPipeActivator]
Net.Tcp Listener Adapter [NetTcpActivator]
```

... continues on next page ...

... continued from previous page ...

```
Net.Tcp Port Sharing Service [NetTcpPortSharing]
Office 64 Source Engine [ose64]
Office Software Protection Platform [osppsvc]
BranchCache [PeerDistSvc]
Hôte de DLL de compteur de performance [PerfHost]
Journaux & alertes de performance [pla]
Service de publication des noms d[U+0092]ordinateurs PNRP [PNRPAutoReg]
Agent de stratégie IPsec [PolicyAgent]
Expérience audio-vidéo haute qualité Windows [QWAVE]
Gestionnaire de connexion automatique d[U+0092]accès distant [RasAuto]
Gestionnaire de connexions d[U+0092]accès distant [RasMan]
Routage et accès distant [RemoteAccess]
Localisateur d[U+0092]appels de procédure distante (RPC) [RpcLocator]
Carte à puce [SCardSvr]
Stratégie de retrait de la carte à puce [SCPolicySvc]
Sauvegarde Windows [SDRSVC]
Ouverture de session secondaire [seclogon]
Brillance adaptative [SensrSvc]
Configuration des services Bureau à distance [SessionEnv]
Partage de connexion Internet (ICS) [SharedAccess]
Interruption SNMP [SNMPTRAP]
Protection logicielle [sppsvc]
Service de notification SPP [sppuinotify]
Service SSTP (Secure Socket Tunneling Protocol) [SstpSvc]
Fournisseur de cliché instantané de logiciel Microsoft [swprv]
Superfetch [SysMain]
Service Panneau de saisie Tablet PC [TabletInputService]
Téléphonie [TapiSrv]
Services de base de module de plateforme sécurisée [TBS]
Services Bureau à distance [TermService]
Serveur de priorités des threads [THREADORDER]
Détection de services interactifs [UI0Detect]
Redirecteur de port du mode utilisateur des services Bureau à distance [UmRdpSer
↪vice]
Gestionnaire d[U+0092]informations d[U+0092]identification [VaultSvc]
Disque virtuel [vds]
Cliché instantané des volumes [VSS]
Temps Windows [W32Time]
Service Windows Activation Technologies [WatAdminSvc]
Service de moteur de sauvegarde en mode bloc [wbengine]
Service de biométrie Windows [WbioSrvc]
Windows Connect Now - Registre de configuration [wcncsvc]
Système de couleurs Windows [WcsPlugInService]
Hôte système de diagnostics [WdiSystemHost]
WebClient [WebClient]
Collecteur d[U+0092]événements de Windows [Wecsvc]
Prise en charge de l[U+0092]application Rapports et solutions aux problèmes du Panneau
```

... continues on next page ...

... continued from previous page ...

```
↪de configuration [wercplsupport]
Service de rapport d[U+0092]erreurs Windows [WerSvc]
Gestion à distance de Windows (Gestion WSM) [WinRM]
Carte de performance WMI [wmiApSrv]
Parental Controls [WPCSvc]
Service Énumérateur d[U+0092]appareil mobile [WPDBusEnum]
Windows Driver Foundation - Infrastructure de pilote mode-utilisateur [wudfsvc]
Service de configuration automatique WWAN [WwanSvc]
################################################
WIN32 active drivers:
Pilote ACPI Microsoft [ACPI]
Ancillary Function Driver for Winsock [AFD]
amdkmdag [amdkmdag]
amdkmdap [amdkmdap]
amdxata [amdxata]
Pilote de média asynchrone RAS [AsyncMac]
Canal IDE [atapi]
Qualcomm Atheros Extensible Wireless LAN device driver [athr]
AMD Function Driver for HD Audio Service [AtiHDAudioService]
Beep [Beep]
blbdrive [blbdrive]
Pilote de prise en charge du navigateur [bowser]
Pilote de CD-ROM [cdrom]
Journal commun (CLFS) [CLFS]
Pilote pour Batterie à méthode de contrôle ACPI Microsoft [CmBatt]
CNG [CNG]
Pilote de batterie composite Microsoft [Compbatt]
Pilote de l[U+0092]énumérateur de bus composite [CompositeBus]
Pilote Fichiers hors connexion [CSC]
DFS Namespace Client Driver [DfsC]
System Attribute Cache [discache]
Pilote de disque [Disk]
LDDM Graphics Subsystem [DXGKrnl]
File Information FS MiniFilter [FileInfo]
FltMgr [FltMgr]
Pilote de filtre de Chiffrement de lecteur Bitlocker [fvevol]
Pilote de fonction UAA 1.1 Microsoft pour le service High Definition Audio [HdAu
↪dAddService]
Pilote de bus UAA Microsoft pour High Definition Audio [HDAudBus]
Intel(R) Management Engine Interface [HECIx64]
Pilote de classe HID Microsoft [HidUsb]
HTTP [HTTP]
Hardware Policy Driver [hwpolicy]
Pilote pour clavier i8042 et souris sur port PS/2 [i8042prt]
Intel HAXM Service [IntelHaxm]
Pilote de processeur Intel [intelppm]
Pilote de la classe Clavier [kbdclass]
```

... continues on next page ...

... continued from previous page ...

```
Pilote HID de clavier [kbdhid]
KSecDD [KSecDD]
KSecPkg [KSecPkg]
Kernel Streaming Thunks [ksthunk]
Link-Layer Topology Discovery Mapper I/O Driver [lltdio]
Virtualisation de fichier UAC [luafv]
Service Pilote de fonction de classe Moniteur Microsoft [monitor]
Pilote de la classe Souris [mouclass]
Pilote HID de souris [mouhid]
Gestionnaire des points de montage [mountmgr]
Pilote d[U+0092]autorisation du Pare-feu Windows [mpsdrv]
Wrapper et moteur de mini-redirecteur SMB [mrxsmb]
Mini-redirecteur SMB 1.x [mrxsmb10]
Mini-redirecteur SMB 2.0 [mrxsmb20]
msahci [msahci]
Msfs [Msfs]
msisadrv [msisadrv]
Pilote BIOS de gestion de systèmes Microsoft [mssmbios]
Mup [Mup]
NativeWiFi Filter [NativeWifiP]
Pilote système NDIS [NDIS]
Pilote TAPI NDIS d[U+0092]accès distant [NdisTapi]
NDIS Usermode I/O Protocol [Ndisuio]
Pilote réseau étendu NDIS d[U+0092]accès distant [NdisWan]
NDIS Proxy [NDProxy]
NetBIOS Interface [NetBIOS]
NetBT [NetBT]
Npfs [Npfs]
NSI proxy service driver. [nsiproxy]
Ntfs [Ntfs]
Null [Null]
Gestionnaire de partitions [partmgr]
Pilote de bus PCI [pci]
Performance Counters for Windows Driver [pcw]
################################################
```

Solution
To prevent access to the services and drivers list, you should either have tight login restrictions, so that only trusted users can access your host, and/or you should filter incoming traffic to this port.

Log Method
Details:SMB Enumerate Services
OID:1.3.6.1.4.1.25623.1.0.102016
Version used: $Revision: 44 $

Log (CVSS: 0.0)
NVT: SMB log in

Summary
This script attempts to logon into the remote host using login/password credentials.

Vulnerability Detection Result
`It was possible to log into the remote host using the SMB protocol.`

Log Method
Details:`SMB log in`
OID:1.3.6.1.4.1.25623.1.0.10394
Version used: `$Revision: 1860 $`

Log (CVSS: 0.0)
NVT: SMB on port 445

Summary
This script detects wether port 445 and 139 are open and if thet are running SMB servers.

Vulnerability Detection Result
`A CIFS server is running on this port`

Log Method
Details:`SMB on port 445`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `$Revision: 41 $`

Log (CVSS: 0.0)
NVT: Microsoft Windows SMB Accessible Shares

Summary
The script detects the Windows SMB Accessible Shares and sets the result into KB.

Vulnerability Detection Result
```
The following shares where found
C$
ADMIN$
IPC$
```

Log Method
Details:`Microsoft Windows SMB Accessible Shares`
OID:1.3.6.1.4.1.25623.1.0.902425
Version used: `$Revision: 977 $`

[return to 192.168.1.25]

2.1.10 Log general/SMBClient

Log (CVSS: 0.0) NVT: SMB Test
Summary Test remote host SMB Functions

Vulnerability Detection Result
`OS Version = WINDOWS 7 ULTIMATE 7601 SERVICE PACK 1`
`Domain = WORKGROUP`
`SMB Serverversion = WINDOWS 7 ULTIMATE 6.1`

Log Method Details:`SMB Test` OID:1.3.6.1.4.1.25623.1.0.90011 Version used: `$Revision: 16 $`

[return to 192.168.1.25]

2.1.11 Log 554/tcp

Log (CVSS: 0.0) NVT: Identify unknown services with nmap
Summary This plugin performs service detection by launching nmap's service probe against ports running unidentified services. Description :

Vulnerability Detection Result
`Nmap service detection result for this port: rtsp`
`This is a guess. A confident identification of the service was not possible.`

Log Method Details:`Identify unknown services with nmap` OID:1.3.6.1.4.1.25623.1.0.66286 Version used: `$Revision: 329 $`

[return to 192.168.1.25]