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 “ubuntuScan”. The scan started at Wed Nov 11 19:12:10 2015 UTC and ended at Wed Nov 11 19:21:12 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
192.168.1.10 blackyfox-easynote-lm86.home	14	2	2	34	0
Total: 1	14	2	2	34	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 52 results selected by the filtering described above. Before filtering there were 54 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.1.10 - blackyfox-easynote-lm86.home	SSH	Success	Protocol SSH, Port 22, User boby

2 Results per Host

2.1 192.168.1.10

Host scan start	Wed Nov 11 19:12:21 2015 UTC
Host scan end	Wed Nov 11 19:21:12 2015 UTC

Service (Port)	Threat Level
general/tcp	High
general/tcp	Medium
general/tcp	Low
22/tcp	Log
general/icmp	Log
general/CPE-T	Log
general/tcp	Log

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities Sep15 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 11.2.202.508
Fixed version:     11.2.202.521
```

Impact
Successful exploitation will allow remote attackers to gain access to potentially sensitive information, conduct denial of service attack and potentially execute arbitrary code in the context of the affected user.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.521 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.521 on Linux.

Vulnerability Insight
Multiple flaws exist due to, - Multiple memory corruption errors. - Multiple unspecified errors. - Multiple use-after-free vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities Sep15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805742
Version used: `$Revision: 1831 $`

References

```
CVE: CVE-2015-5567, CVE-2015-5568, CVE-2015-5570, CVE-2015-5571, CVE-2015-5572,
↪CVE-2015-5573, CVE-2015-5574, CVE-2015-5575, CVE-2015-5576, CVE-2015-5577, CVE
↪-2015-5578, CVE-2015-5579, CVE-2015-5580, CVE-2015-5581, CVE-2015-5582, CVE-20
↪15-5584, CVE-2015-5587, CVE-2015-5588, CVE-2015-6676, CVE-2015-6677, CVE-2015-
↪6678, CVE-2015-6679, CVE-2015-6682
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb15-23.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - 01 Oct15 (Linux)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 11.2.202.508
Fixed version:     11.2.202.535
```

Impact

Successful exploitation will allow attackers to obtain sensitive information, execute arbitrary code or cause a denial of service and have other unspecified impacts.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.535 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player before version 11.2.202.535 on Linux.

Vulnerability Insight

Multiple flaws exists due to, - Improper implementation of the Flash broker API. - Multiple memory corruption errors. - An use-after-free error. - An error in same origin policy. - A buffer overflow error.

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities - 01 Oct15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806095
Version used: `$Revision: 1962 $`

References

```
CVE: CVE-2015-5569, CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7628,
↪CVE-2015-7629, CVE-2015-7630, CVE-2015-7631, CVE-2015-7632, CVE-2015-7633, CVE
↪-2015-7634, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-20
↪15-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, CVE-2015-
↪7644
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb15-25.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Unspecified Vulnerability Oct15 (Linux)

Summary

This host is installed with Adobe Flash Player and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 11.2.202.508
Fixed version:  11.2.202.540
```

Impact

Successful exploitation will allow attackers to cause a crash and potentially an attacker to take control of the affected system.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.540 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player versions 11.x through 11.2.202.535 on Linux.

Vulnerability Insight

The flaw is due to some unspecified critical vulnerabilities in Adobe Flash Player.

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Unspecified Vulnerability Oct15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806500
Version used: `$Revision: 1980 $`

References

```
CVE: CVE-2015-7645, CVE-2015-7647, CVE-2015-7648
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsa15-05.html
   URL:https://helpx.adobe.com/security/products/flash-player/apsb15-27.html
   URL:http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flas
↪h-zero-day-used-in-pawn-storm-campaign
```

High (CVSS: 10.0)
NVT: Ubuntu Update for freetype USN-2739-1

Summary

Check the version of freetype

Vulnerability Detection Result

```
Package libfreetype6:amd64 version 2.5.2-1ubuntu2.4 is installed which is known
↪to be vulnerable.
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
freetype on Ubuntu 14.04 LTS , Ubuntu 12.04 LTS

Vulnerability Insight
It was discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or hang, resulting in a denial of service, or possibly expose uninitialized memory.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check if the version is vulnerable or not.
Details:`Ubuntu Update for freetype USN-2739-1`
OID:1.3.6.1.4.1.25623.1.0.842436
Version used: `$Revision: 1712 $`

References

```
Other:
  USN:2739-1
   URL:https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-September
↪/003111.html
```

High (CVSS: 10.0)
NVT: Ubuntu Update for icu USN-2740-1

Summary
Check the version of icu

Vulnerability Detection Result

```
Package libicu52:amd64 version 52.1-3ubuntu0.3 is installed which is known to be
↪ vulnerable.
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
icu on Ubuntu 14.04 LTS , Ubuntu 12.04 LTS

Vulnerability Insight
Atte Kettunen discovered that ICU incorrectly handled certain converter names. If an application using ICU processed crafted data, a remote attacker could possibly cause it to crash. (CVE-2015-1270)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that ICU incorrectly handled certain memory operations when processing data. If an application using ICU processed crafted data, a remote attacker could possibly cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program. (CVE-2015-2632, CVE-2015-4760)

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check if the version is vulnerable or not.
Details:`Ubuntu Update for icu USN-2740-1`
OID:1.3.6.1.4.1.25623.1.0.842437
Version used: `$Revision: 1798 $`

References

```
CVE: CVE-2015-1270, CVE-2015-2632, CVE-2015-4760
Other:
  USN:2740-1
   URL:https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-September
↪/003114.html
```

High (CVSS: 10.0)
NVT: Ubuntu Update for oxide-qt USN-2757-1

Summary

Check the version of oxide-qt

Vulnerability Detection Result

```
Package liboxideqtcore0:amd64 version 1.8.4-0ubuntu0.14.04.2 is installed which
↪is known to be vulnerable.
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

oxide-qt on Ubuntu 15.04 , Ubuntu 14.04 LTS

Vulnerability Insight

Two security issues were discovered in Blink and V8. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to bypass same-origin restrictions. (CVE-2015-1303, CVE-2015-1304)

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check if the version is vulnerable or not.
Details:`Ubuntu Update for oxide-qt USN-2757-1`
OID:1.3.6.1.4.1.25623.1.0.842477

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 1899 $`

References

```
CVE: CVE-2015-1303, CVE-2015-1304
Other:
  USN:2757-1
   URL:https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-October/0
↪03136.html
```

High (CVSS: 10.0)
NVT: Ubuntu Update for spice USN-2766-1

Summary

Check the version of spice

Vulnerability Detection Result

```
Package libspice-server1:amd64 version 0.12.4-0nocelt2ubuntu1 is installed which
↪ is known to be vulnerable.
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

spice on Ubuntu 15.04 , Ubuntu 14.04 LTS

Vulnerability Insight

Frediano Ziglio discovered multiple buffer overflows, undefined behavior signed integer operations, race conditions, memory leaks, and denial of service issues in Spice. A malicious guest operating system could potentially exploit these issues to escape virtualization. (CVE-2015-5260, CVE-2015-5261)

Vulnerability Detection Method

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

Details:`Ubuntu Update for spice USN-2766-1`

OID:1.3.6.1.4.1.25623.1.0.842485

Version used: `$Revision: 1899 $`

References

```
CVE: CVE-2015-5260, CVE-2015-5261
Other:
  USN:2766-1
   URL:https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-October/0
↪03144.html
```

High (CVSS: 9.3)
NVT: Ubuntu Update for firefox USN-2743-1

Summary
Check the version of firefox

Vulnerability Detection Result

```
Package firefox version 40.0.3+build1-0ubuntu0.14.04.1 is installed which is kno
↪wn to be vulnerable.
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
firefox on Ubuntu 15.04 , Ubuntu 14.04 LTS , Ubuntu 12.04 LTS

Vulnerability Insight
Andrew Osmond, Olli Pettay, Andrew Sutherland, Christian Holler, David Major, Andrew McCreight, Cameron McCormack, Bob Clary and Randell Jesup discovered multiple memory safety issues in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4500, CVE-2015-4501)
Andr
233 Bargull discovered that when a web page creates a scripted proxy for the window with a handler defined a certain way, a reference to the inner window will be passed, rather than that of the outer window. (CVE-2015-4502)
Felix Gr
246 bert discovered an out-of-bounds read in the QCMS color management library in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or obtain sensitive information. (CVE-2015-4504)
Khalil Zhani discovered a buffer overflow when parsing VP9 content in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4506)
Spandan Veggalam discovered a crash while using the debugger API in some circumstances. If a user were tricked in to opening a specially crafted website whilst using the debugger, an attacker could potentially exploit this to execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4507)
Juho Nurminen discovered that the URL bar could display the wrong URL in reader mode in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to conduct URL spoofing attacks. (CVE-2015-4508)
A use-after-free was discovered when manipulating HTML media content in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4509)

. . . continues on next page . . .

. . . continued from previous page . . .

Looben Yang discovered a use-after-free when using a shared worker with IndexedDB in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the pr ...
Description truncated, for more information please check the Reference URL

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check if the version is vulnerable or not.
Details:`Ubuntu Update for firefox USN-2743-1`
OID:1.3.6.1.4.1.25623.1.0.842456
Version used: `$Revision: 1858 $`

References

```
CVE: CVE-2015-4500, CVE-2015-4501, CVE-2015-4502, CVE-2015-4504, CVE-2015-4506,
↪CVE-2015-4507, CVE-2015-4508, CVE-2015-4509, CVE-2015-4510, CVE-2015-4512, CVE
↪-2015-4516, CVE-2015-4517, CVE-2015-4521, CVE-2015-4522, CVE-2015-7174, CVE-20
↪15-7175, CVE-2015-7176, CVE-2015-7177, CVE-2015-7180, CVE-2015-4519, CVE-2015-
↪4520
Other:
  USN:2743-1
   URL:https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-September
↪/003115.html
```

High (CVSS: 9.3)
NVT: Ubuntu Update for ubufox USN-2743-2

Summary
Check the version of ubufox

Vulnerability Detection Result

```
Package xul-ext-ubufox version 3.1-0ubuntu0.14.04.1 is installed which is known
↪to be vulnerable.
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
ubufox on Ubuntu 15.04 , Ubuntu 14.04 LTS , Ubuntu 12.04 LTS

Vulnerability Insight
USN-2743-1 fixed vulnerabilities in Firefox. This update provides the corresponding update for Ubufox.
Original advisory details:

. . . continues on next page . . .

. . . continued from previous page . . .

Andrew Osmond, Olli Pettay, Andrew Sutherland, Christian Holler, David Major, Andrew McCreight, Cameron McCormack, Bob Clary and Randell Jesup discovered multiple memory safety issues in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4500, CVE-2015-4501)
Andr
233 Bargull discovered that when a web page creates a scripted proxy for the window with a handler defined a certain way, a reference to the inner window will be passed, rather than that of the outer window. (CVE-2015-4502)
Felix Gr
246 bert discovered an out-of-bounds read in the QCMS color management library in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or obtain sensitive information. (CVE-2015-4504)
Khalil Zhani discovered a buffer overflow when parsing VP9 content in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4506)
Spandan Veggalam discovered a crash while using the debugger API in some circumstances. If a user were tricked in to opening a specially crafted website whilst using the debugger, an attacker could potentially exploit this to execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4507)
Juho Nurminen discovered that the URL bar could display the wrong URL in reader mode in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to conduct URL spoofing attacks. (CVE-2015-4508)
A use-after-free was discovered when manipulating HTML media content in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4509)
Looben Yang discovered a use-after-free when using a shared worker with IndexedDB in some circumstances. If a user were tricked in to opening a specially crafted website, a ...
Description truncated, for more information please check the Reference URL

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check if the version is vulnerable or not.
Details:`Ubuntu Update for ubufox USN-2743-2`
OID:1.3.6.1.4.1.25623.1.0.842457
Version used: `$Revision: 1858 $`

References

```
CVE: CVE-2015-4500, CVE-2015-4501, CVE-2015-4502, CVE-2015-4504, CVE-2015-4506,
↪CVE-2015-4507, CVE-2015-4508, CVE-2015-4509, CVE-2015-4510, CVE-2015-4512, CVE
↪-2015-4516, CVE-2015-4517, CVE-2015-4521, CVE-2015-4522, CVE-2015-7174, CVE-20
↪15-7175, CVE-2015-7176, CVE-2015-7177, CVE-2015-7180, CVE-2015-4519, CVE-2015-
↪4520
Other:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  USN:2743-2
   URL:https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-September
↪/003116.html
```

High (CVSS: 9.3)
NVT: Ubuntu Update for unity-firefox-extension USN-2743-3

Summary
Check the version of unity-firefox-extension

Vulnerability Detection Result

```
Package xul-ext-unity version 3.0.0+14.04.20140416-0ubuntu1 is installed which i
↪s known to be vulnerable.
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
unity-firefox-extension on Ubuntu 15.04 , Ubuntu 14.04 LTS

Vulnerability Insight
USN-2743-1 fixed vulnerabilities in Firefox. Future Firefox updates will require all addons be signed and unity-firefox-extension, webapps-greasemonkey and webaccounts-browser-extension will not go through the signing process. Because these addons currently break search engine installations (LP: 1069793), this update permanently disables the addons by removing them from the system.
We apologize for any inconvenience.
Original advisory details:
Andrew Osmond, Olli Pettay, Andrew Sutherland, Christian Holler, David Major, Andrew McCreight, Cameron McCormack, Bob Clary and Randell Jesup discovered multiple memory safety issues in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4500, CVE-2015-4501)
Andr
233 Bargull discovered that when a web page creates a scripted proxy for the window with a handler defined a certain way, a reference to the inner window will be passed, rather than that of the outer window. (CVE-2015-4502)
Felix Gr
246 bert discovered an out-of-bounds read in the QCMS color management library in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or obtain sensitive information. (CVE-2015-4504)
Khalil Zhani discovered a buffer overflow when parsing VP9 content in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4506)

. . . continues on next page . . .

. . . continued from previous page . . .

Spandan Veggalam discovered a crash while using the debugger API in some circumstances. If a user were tricked in to opening a specially crafted website whilst using the debugger, an attacker could potentially exploit this to execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4507)
Juho Nurminen discovered that the URL bar could display the wrong URL in reader mode in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to conduct URL spoofing attacks. (CVE-2015-4508)
A use-after-free was discovered when manipulating HTML media content in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this t ...
Description truncated, for more information please check the Reference URL

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check if the version is vulnerable or not.
Details:`Ubuntu Update for unity-firefox-extension USN-2743-3`
OID:1.3.6.1.4.1.25623.1.0.842460
Version used: `$Revision: 1848 $`

References

```
CVE: CVE-2015-4500, CVE-2015-4501, CVE-2015-4502, CVE-2015-4504, CVE-2015-4506,
↪CVE-2015-4507, CVE-2015-4508, CVE-2015-4509, CVE-2015-4510, CVE-2015-4512, CVE
↪-2015-4516, CVE-2015-4517, CVE-2015-4521, CVE-2015-4522, CVE-2015-7174, CVE-20
↪15-7175, CVE-2015-7176, CVE-2015-7177, CVE-2015-7180, CVE-2015-4519, CVE-2015-
↪4520
Other:
  USN:2743-3
   URL:https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-September
↪/003118.html
```

High (CVSS: 9.3)
NVT: Ubuntu Update for firefox USN-2743-4

Summary
Check the version of firefox

Vulnerability Detection Result

```
Package firefox version 40.0.3+build1-0ubuntu0.14.04.1 is installed which is kno
↪wn to be vulnerable.
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
firefox on Ubuntu 15.04 , Ubuntu 14.04 LTS , Ubuntu 12.04 LTS

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

USN-2743-1 fixed vulnerabilities in Firefox. After upgrading, some users reported problems with bookmark creation and crashes in some circumstances. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Andrew Osmond, Olli Pettay, Andrew Sutherland, Christian Holler, David Major, Andrew McCreight, Cameron McCormack, Bob Clary and Randell Jesup discovered multiple memory safety issues in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4500, CVE-2015-4501)
Andr
233 Bargull discovered that when a web page creates a scripted proxy for the window with a handler defined a certain way, a reference to the inner window will be passed, rather than that of the outer window. (CVE-2015-4502)
Felix Gr
246 bert discovered an out-of-bounds read in the QCMS color management library in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or obtain sensitive information. (CVE-2015-4504)
Khalil Zhani discovered a buffer overflow when parsing VP9 content in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4506)
Spandan Veggalam discovered a crash while using the debugger API in some circumstances. If a user were tricked in to opening a specially crafted website whilst using the debugger, an attacker could potentially exploit this to execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4507)
Juho Nurminen discovered that the URL bar could display the wrong URL in reader mode in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to conduct URL spoofing attacks. (CVE-2015-4508)
A use-after-free was discovered when manipulating HTML media content in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2015-4509)
Looben Yang discovered a use-after-free when using a shar ...
Description truncated, for more information please check the Reference URL

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check if the version is vulnerable or not.
Details:`Ubuntu Update for firefox USN-2743-4`
OID:1.3.6.1.4.1.25623.1.0.842476
Version used: `$Revision: 1899 $`

References

`CVE: CVE-2015-4500, CVE-2015-4501, CVE-2015-4502, CVE-2015-4504, CVE-2015-4506,`

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪CVE-2015-4507, CVE-2015-4508, CVE-2015-4509, CVE-2015-4510, CVE-2015-4512, CVE
↪-2015-4516, CVE-2015-4517, CVE-2015-4521, CVE-2015-4522, CVE-2015-7174, CVE-20
↪15-7175, CVE-2015-7176, CVE-2015-7177, CVE-2015-7180, CVE-2015-4519, CVE-2015-
↪4520
Other:
  USN:2743-4
   URL:https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-October/0
↪03135.html
```

High (CVSS: 7.5)
NVT: Ubuntu Update for oxide-qt USN-2735-1

Summary
Check the version of oxide-qt

Vulnerability Detection Result

```
Package liboxideqtcore0:amd64 version 1.8.4-0ubuntu0.14.04.2 is installed which
↪is known to be vulnerable.
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
oxide-qt on Ubuntu 14.04 LTS

Vulnerability Insight
It was discovered that the DOM tree could be corrupted during parsing in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to bypass same-origin restrictions or cause a denial of service. (CVE-2015-1291)
An issue was discovered in NavigatorServiceWorker::serviceWorker in Blink. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to bypass same-origin restrictions. (CVE-2015-1292)
An issue was discovered in the DOM implementation in Blink. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to bypass same-origin restrictions. (CVE-2015-1293)
A use-after-free was discovered in Skia. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via renderer crash, or execute arbitrary code with the privileges of the sandboxed render process. (CVE-2015-1294)
A use-after-free was discovered in the shared-timer implementation in Blink. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via renderer crash, or execute arbitrary code with the privileges of the sandboxed render process. (CVE-2015-1299)
It was discovered that the availability of iframe Resource Timing API times was not properly restricted in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to obtain sensitive information. (CVE-2015-1300)

. . . continues on next page . . .

. . . continued from previous page . . .

Multiple security issues were discovered in Chromium. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to read uninitialized memory, cause a denial of service via application crash or execute arbitrary code with the privileges of the user invoking the program. (CVE-2015-1301)
A heap corruption issue was discovered in oxide::JavaScriptDialogManager. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking the program. (CVE-2015-1332)

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check if the version is vulnerable or not.
Details:`Ubuntu Update for oxide-qt USN-2735-1`
OID:1.3.6.1.4.1.25623.1.0.842433
Version used: `$Revision: 1712 $`

References

```
CVE: CVE-2015-1291, CVE-2015-1292, CVE-2015-1293, CVE-2015-1294, CVE-2015-1299,
↪CVE-2015-1300, CVE-2015-1301, CVE-2015-1332
Other:
  USN:2735-1
   URL:https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-September
↪/003108.html
```

High (CVSS: 7.5)
NVT: Ubuntu Update for thunderbird USN-2754-1

Summary
Check the version of thunderbird

Vulnerability Detection Result

```
Package thunderbird version 38.2.0+build1-0ubuntu0.14.04.1 is installed which is
↪ known to be vulnerable.
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
thunderbird on Ubuntu 15.04 , Ubuntu 14.04 LTS , Ubuntu 12.04 LTS

Vulnerability Insight
Andrew Osmond, Olli Pettay, Andrew Sutherland, Christian Holler, David Major, Andrew McCreight, and Cameron McCormack discovered multiple memory safety issues in Thunderbird. If a user were tricked in to opening a specially crafted message, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2015-4500)

. . . continues on next page . . .

. . . continued from previous page . . .

Khalil Zhani discovered a buffer overflow when parsing VP9 content in some circumstances. If a user were tricked in to opening a specially crafted message, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2015-4506)

A use-after-free was discovered when manipulating HTML media content in some circumstances. If a user were tricked in to opening a specially crafted website in a browsing context, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2015-4509)

Atte Kettunen discovered a buffer overflow in the nestegg library when decoding WebM format video in some circumstances. If a user were tricked in to opening a specially crafted message, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2015-4511)

Ronald Crane reported multiple vulnerabilities. If a user were tricked in to opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2015-4517, CVE-2015-4521, CVE-2015-4522, CVE-2015-7174, CVE-2015-7175, CVE-2015-7176, CVE-2015-7177, CVE-2015-7180)

Mario Gomes discovered that dragging and dropping an image after a redirect exposes the redirected URL to scripts. An attacker could potentially exploit this to obtain sensitive information. (CVE-2015-4519)

Ehsan Akhgari discovered 2 issues with CORS preflight requests. An attacker could potentially exploit these to bypass CORS restrictions. (CVE-2015-4520)

Vulnerability Detection Method

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

Details:`Ubuntu Update for thunderbird USN-2754-1`

OID:1.3.6.1.4.1.25623.1.0.842482

Version used: `$Revision: 1899 $`

References

```
CVE: CVE-2015-4500, CVE-2015-4506, CVE-2015-4509, CVE-2015-4511, CVE-2015-4517,
↪CVE-2015-4521, CVE-2015-4522, CVE-2015-7174, CVE-2015-7175, CVE-2015-7176, CVE
↪-2015-7177, CVE-2015-7180, CVE-2015-4519, CVE-2015-4520
Other:
  USN:2754-1
   URL:https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-October/0
↪03137.html
```

High (CVSS: 7.2)

NVT: Ubuntu Update for apport USN-2744-1

Summary

Check the version of apport

Vulnerability Detection Result

```
Package apport version 2.14.1-0ubuntu3.12 is installed which is known to be vuln
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪erable.
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

apport on Ubuntu 15.04 , Ubuntu 14.04 LTS , Ubuntu 12.04 LTS

Vulnerability Insight

Halfdog discovered that Apport incorrectly handled kernel crash dump files. A local attacker could use this issue to cause a denial of service, or possibly elevate privileges. The default symlink protections for affected releases should reduce the vulnerability to a denial of service.

Vulnerability Detection Method

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

Details:`Ubuntu Update for apport USN-2744-1`

OID:1.3.6.1.4.1.25623.1.0.842461

Version used: `$Revision: 1935 $`

References

```
CVE: CVE-2015-1338
Other:
  USN:2744-1
   URL:https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-September
↪/003117.html
```

[return to 192.168.1.10]

2.1.2 Medium general/tcp

Medium (CVSS: 6.9)

NVT: Ubuntu Update for spice USN-2736-1

Summary

Check the version of spice

Vulnerability Detection Result

```
Package libspice-server1:amd64 version 0.12.4-0nocelt2ubuntu1 is installed which
↪ is known to be vulnerable.
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
spice on Ubuntu 14.04 LTS

Vulnerability Insight
Frediano Ziglio discovered that Spice incorrectly handled monitor configs. A malicious guest could use this issue to cause a denial of service, or possibly execute arbitrary code on the host as the user running the QEMU process. In the default installation, when QEMU is used with libvirt, attackers would be isolated by the libvirt AppArmor profile.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check if the version is vulnerable or not.
Details:`Ubuntu Update for spice USN-2736-1`
OID:1.3.6.1.4.1.25623.1.0.842434
Version used: `$Revision: 1729 $`

References

```
CVE: CVE-2015-3247
Other:
  USN:2736-1
   URL:https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-September
↪/003107.html
```

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

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

Vulnerability Detection Result

```
Installed version: 2.1.6
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
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 Linux.

. . . continues on next page . . .

. . . continued from previous page . . .

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806087
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
```

[return to 192.168.1.10]

2.1.3 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary

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: 54254
Paket 2: 54513
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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
```

Low (CVSS: 2.1)

NVT: Ubuntu Update for unity-settings-daemon USN-2741-1

Summary

Check the version of unity-settings-daemon

Vulnerability Detection Result

```
Package unity-settings-daemon version 14.04.0+14.04.20140606-0ubuntu3 is install
↪ed which is known to be vulnerable.
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

unity-settings-daemon on Ubuntu 14.04 LTS

Vulnerability Insight

It was discovered that the Unity Settings Daemon incorrectly allowed removable media to be mounted when the screen is locked. If a vulnerability were discovered in some other desktop component, such as an image library, a local attacker could possibly use this issue to gain access to the session.

Vulnerability Detection Method

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

Details:`Ubuntu Update for unity-settings-daemon USN-2741-1`

OID:1.3.6.1.4.1.25623.1.0.842438

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 1858 $`

References

```
CVE: CVE-2015-1319
Other:
  USN:2741-1
   URL:https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-September
↪/003112.html
```

[return to 192.168.1.10]

2.1.4 Log 22/tcp

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported

Summary

Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
SSHv2 Fingerprint:
ssh-rsa: 3b:a0:ca:6d:6a:3b:31:bd:fd:3d:c5:7e:2e:0e:b7:8f
ssh-dss: 78:61:24:d7:f4:e0:b7:b3:0c:9a:25:2e:e0:7d:ed:ad
ecdsa-sha2-nistp256: 35:ab:29:2d:04:a3:82:81:af:78:86:9f:87:e2:1c:9a
```

Log Method

Details:`SSH Protocol Versions Supported`
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: `$Revision: 1952 $`

Log (CVSS: 0.0)
NVT: SSH Server type and version

Summary

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Detected SSH server version: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
Remote SSH supported authentication: password,publickey
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:6.6.1p1
Concluded from remote connection attempt with credentials:
  Login: OpenVAS
  Password: OpenVAS
```

Log Method

Details:`SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `$Revision: 1789 $`

Log (CVSS: 0.0)
NVT: Services

Summary

This plugin attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 and set the results in the plugins knowledge base.

Vulnerability Detection Result

```
An ssh server is running on this port
```

Log Method

Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 69 $`

Log (CVSS: 0.0)
NVT: Determine OS and list of installed packages via SSH login

Summary

This script will, if given a userid/password or key to the remote system, login to that system, determine the OS it is running, and for supported systems, extract the list of installed packages/rpms.

Vulnerability Detection Result

```
We are able to login and detect that you are running Ubuntu 14.04 LTS
```

Vulnerability Insight

The ssh protocol is used to log in. If a specific port is configured for the credential, then only this port will be tried. Else any port that offers ssh, usually port 22.

. . . continues on next page . . .

. . . continued from previous page . . .

Upon successful login, the command 'uname -a' is issued to find out about the type amd version of the operating system.
The result is analysed for various patterns and in several cases additional commands are tried to find out more details and to confirm a detection.
The regular Linux distributions are detected this way as well as other linunxoid systems and also many Linux-based devices and appliances.
If the system offers a package database, for example RPM- or DEB-based, this full list of installed packages is retrieved for further patch-level checks.

Log Method

Details:`Determine OS and list of installed packages via SSH login`
OID:1.3.6.1.4.1.25623.1.0.50282
Version used: `$Revision: 1981 $`

Log (CVSS: 0.0)
NVT: SSH Authorization Check

Summary

This script tries to login with provided credentials.
If the login was successful, it marks this port as available for any authenticated tests.

Vulnerability Detection Result

```
It was possible to login using the provided SSH credentials.
Hence authenticated checks are enabled.
```

Log Method

Details:`SSH Authorization Check`
OID:1.3.6.1.4.1.25623.1.0.90022
Version used: `$Revision: 948 $`

[return to 192.168.1.10]

2.1.5 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary

The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability was detected according to the Vulnerability Detection Method.

Log Method

Details:`ICMP Timestamp Detection`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `$Revision: 13 $`

References

```
CVE: CVE-1999-0524
Other:
  URL:http://www.ietf.org/rfc/rfc0792.txt
```

[return to 192.168.1.10]

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

```
192.168.1.10|cpe:/a:libreoffice:libreoffice:4.2.8.2.2
192.168.1.10|cpe:/a:hp:hplip:3.14.3
192.168.1.10|cpe:/a:openssl:openssl:1.0.1f
192.168.1.10|cpe:/a:wireshark:wireshark:1.10.6
192.168.1.10|cpe:/a:mozilla:thunderbird:38.2.0
192.168.1.10|cpe:/a:mozilla:firefox:40.0.3
192.168.1.10|cpe:/a:libpng:libpng:1.2.50
192.168.1.10|cpe:/a:videolan:vlc_media_player:2.1.6
192.168.1.10|cpe:/a:gnu:binutils:2.24
192.168.1.10|cpe:/a:isc:dhcp:4.2.4
192.168.1.10|cpe:/a:ruby-lang:ruby:1.9.3.p484:p484
192.168.1.10|cpe:/a:gnu:gcc:4.8
192.168.1.10|cpe:/a:adobe:flash_player:11.2.202.508
192.168.1.10|cpe:/a:openoffice:openoffice.org:3.4.
192.168.1.10|cpe:/a:sun:openjdk:2.5.6.0
192.168.1.10|cpe:/a:avahi:avahi:0.6.31
192.168.1.10|cpe:/a:gnu:gzip:1.6
192.168.1.10|cpe:/a:gnu:gzip:1.2.4
192.168.1.10|cpe:/a:imagemagick:imagemagick:6.7.7.1
192.168.1.10|cpe:/a:sun:jre:1.7.0_79
192.168.1.10|cpe:/a:openbsd:openssh:6.6.1p1
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
192.168.1.10|cpe:/a:ghostscript:ghostscript:9.10
192.168.1.10|cpe:/o:canonical:ubuntu_linux:14.04:-:lts
```

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

[return to 192.168.1.10]

2.1.7 Log general/tcp

Log (CVSS: 0.0)
NVT: OS fingerprinting

Summary
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: (100% confidence)
Linux Kernel
```

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: 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 192.168.1.10:
192.168.1.22
192.168.1.10
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution
Block unwanted packets from escaping your network.

Log Method
Details:`Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `$Revision: 975 $`

Log (CVSS: 0.0)
NVT: Mozilla Firefox Version Detection (Linux)

Summary
This script finds the Mozilla Firefox installed version on Linux and save the version in KB.

Vulnerability Detection Result

```
Detected Firefox
Version: 40.0.3
Location: /usr/bin/firefox
CPE: cpe:/a:mozilla:firefox:40.0.3
Concluded from version identification result:
40.0.3
```

Log Method
Details:`Mozilla Firefox Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800017
Version used: `$Revision: 1098 $`

Log (CVSS: 0.0)
NVT: Mozilla Firefox Version Detection (Linux)

Summary
This script finds the Mozilla Firefox installed version on Linux and save the version in KB.

Vulnerability Detection Result

```
Detected Firefox
Version: 40.0.3
Location: /usr/lib/firefox/firefox
CPE: cpe:/a:mozilla:firefox:40.0.3
Concluded from version identification result:
40.0.3
```

Log Method
Details:`Mozilla Firefox Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800017

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 1098 $`

Log (CVSS: 0.0)
NVT: Mozilla Thunderbird Version Detection (Linux)

Summary
This script retrieves Mozilla ThunderBird Version and saves it in KB.

Vulnerability Detection Result

```
Mozilla Thunderbird version 38.2.0 running at location /usr/bin/thunderbird
 was detected on the host
```

Log Method
Details:`Mozilla Thunderbird Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800018
Version used: `$Revision: 1040 $`

Log (CVSS: 0.0)
NVT: Adobe Flash Player/AIR Version Detection (Linux)

Summary
Detection of installed version of Adobe Flash Player/AIR on Windows.
The script logs in via ssh, extracts the version from the binary file and set it in KB.

Vulnerability Detection Result

```
Detected Adobe Flash Player
Version: 11.2.202.508
Location: /usr/lib/flashplugin-installer/libflashplayer.so
CPE: cpe:/a:adobe:flash_player:11.2.202.508
Concluded from version identification result:
11.2.202.508
```

Log Method
Details:`Adobe Flash Player/AIR Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800032
Version used: `$Revision: 1012 $`

Log (CVSS: 0.0)
NVT: Wireshark Version Detection (Linux)

Summary
Detection of installed version of Wireshark.
The script logs in via ssh, searches for executable 'wireshark' and queries the found executables via command line option '-v'.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Detected Wireshark version: 1.10.6
Location: /usr/bin/wireshark
CPE: cpe:/a:wireshark:wireshark:1.10.6
Concluded from version identification result:
wireshark 1.10.6 (v1.10.6 from master-1.10)
Copyright 1998-2014 Gerald Combs <gerald@wireshark.org> and contributors.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Compiled (64-bit) with GTK+ 3.10.7, with Cairo 1.13.1, with Pango 1.36.1, with
GLib 2.39.91, with libpcap, with libz 1.2.8, with POSIX capabilities (Linux),
without libnl, with SMI 0.4.8, with c-ares 1.10.0, with Lua 5.2, without Python,
with GnuTLS 2.12.23, with Gcrypt 1.5.3, with MIT Kerberos, with GeoIP, with
PortAudio V19-devel (built Feb 25 2014 21:09:53), with AirPcap.
Running on Linux 3.13.0-62-generic, with locale C, with libpcap version 1.5.3,
with libz 1.2.8, GnuTLS 2.12.23, Gcrypt 1.5.3, without AirPcap.
Intel(R) Core(TM) i5 CPU       M 430  @ 2.27GHz
Built using gcc 4.8.2.
```

Log Method

Details:Wireshark Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800039
Version used: $Revision: 1128 $

Log (CVSS: 0.0)
NVT: OpenSSL Version Detection (Linux)

Summary

Detection of installed version of OpenSSL.
The script logs in via ssh, searches for executable ’openssl’ and queries the found executables via command line option ’version’.

Vulnerability Detection Result

```
Detected OpenSSL
Version: 1.0.1f
Location: /usr/bin/openssl
CPE: cpe:/a:openssl:openssl:1.0.1f
Concluded from version identification result:
OpenSSL 1.0.1f 6 Jan 2014
```

Log Method

Details:OpenSSL Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800335
Version used: $Revision: 1128 $

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

Summary

Detection of installed version of Java products on Linux systems. It covers Sun Java, IBM Java and GCJ.
The script logs in via ssh, searches for executables 'javaaws' and 'java' and queries the found executables via command line option '-fullversion'.

Vulnerability Detection Result

```
Detected Sun Java JRE version: 1.7.0_79-b14
Location: /usr/bin/java
Concluded from version identification result:
java full version "1.7.0_79-b14"
```

Log Method

Details:`Sun Java Products Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800385
Version used: `$Revision: 1128 $`

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

Summary

Detection of installed version of Java products on Linux systems. It covers Sun Java, IBM Java and GCJ.
The script logs in via ssh, searches for executables 'javaaws' and 'java' and queries the found executables via command line option '-fullversion'.

Vulnerability Detection Result

```
Detected Sun Java JRE version: 1.7.0_79-b14
Location: /usr/lib/jvm/java-7-openjdk-amd64/bin/java
Concluded from version identification result:
java full version "1.7.0_79-b14"
```

Log Method

Details:`Sun Java Products Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800385
Version used: `$Revision: 1128 $`

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

Summary

Detection of installed version of Java products on Linux systems. It covers Sun Java, IBM Java and GCJ.

. . . continues on next page . . .

. . . continued from previous page . . .

The script logs in via ssh, searches for executables 'javaaws' and 'java' and queries the found executables via command line option '-fullversion'.

Vulnerability Detection Result

```
Detected Sun Java JRE version: 1.7.0_79-b14
Location: /usr/lib/jvm/java-7-openjdk-amd64/jre/bin/java
Concluded from version identification result:
java full version "1.7.0_79-b14"
```

Log Method

Details:`Sun Java Products Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800385
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary

Detection of installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.2.4
Location: /usr/lib/klibc/bin/gzip
CPE: cpe:/a:gnu:gzip:1.2.4
Concluded from version identification result:
gzip 1.2.4 (18 Aug 93)
usage: gzip [-cdfhlLnNtvV19] [-S suffix] [file ...]
 -c --stdout      write on standard output, keep original files unchanged
 -d --decompress  decompress
 -f --force       force overwrite of output file and compress links
 -h --help        give this help
 -L --license     display software license
 -n --no-name     do not save or restore the original name and time stamp
 -N --name        save or restore the original name and time stamp
 -q --quiet       suppress all warnings
 -S .suf  --suffix .suf     use suffix .suf on compressed files
 -t --test        test compressed file integrity
 -v --verbose     verbose mode
 -V --version     display version number
 file...          files to decompress. If none given, use standard input.
```

Log Method

Details:`GZip Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary
Detection of installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.6
Location: /bin/gzip
CPE: cpe:/a:gnu:gzip:1.6
Concluded from version identification result:
gzip 1.6
Copyright (C) 2007, 2010, 2011 Free Software Foundation, Inc.
Copyright (C) 1993 Jean-loup Gailly.
This is free software.  You may redistribute copies of it under the terms of
the GNU General Public License <http://www.gnu.org/licenses/gpl.html>.
There is NO WARRANTY, to the extent permitted by law.
Written by Jean-loup Gailly.
```

Log Method
Details:`GZip Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: GCC Version Detection (Linux)

Summary
Detection of installed version of GCC.
The script logs in via ssh, searches for executable 'gcc' and queries the found executables via command line option '-v'

Vulnerability Detection Result

```
Detected GNU GCC
Version: 4.8
Location: /usr/bin/gcc
CPE: cpe:/a:gnu:gcc:4.8
Concluded from version identification result:
4.8
```

Log Method
Details:`GCC Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806083
Version used: `$Revision: 1970 $`

Log (CVSS: 0.0)
NVT: GCC Version Detection (Linux)

Summary

Detection of installed version of GCC.
The script logs in via ssh, searches for executable 'gcc' and queries the found executables via command line option '-v'

Vulnerability Detection Result

```
Detected GNU GCC
Version: 4.8
Location: /usr/share/doc/gcc-4.8-base/gcc
CPE: cpe:/a:gnu:gcc:4.8
Concluded from version identification result:
4.8
```

Log Method

Details:`GCC Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806083
Version used: `$Revision: 1970 $`

Log (CVSS: 0.0)
NVT: GNU_Assembler Version Detection (Linux)

Summary

This script finds the GNU Assembler installed version on Linux.
The script logs in via ssh, execute the command 'dpkg' and sets the version in KB.

Vulnerability Detection Result

```
Detected GNU assembler
Version: 2.24
Location: /
CPE: cpe:/a:gnu:binutils:2.24
Concluded from version identification result:
2.24
```

Log Method

Details:`GNU_Assembler Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806084
Version used: `$Revision: 1970 $`

Log (CVSS: 0.0)
NVT: GNU Binutils Version Detection (Linux)

Summary

This script finds the GNU Binutils installed version on Linux.

. . . continues on next page . . .

... continued from previous page ...

The script logs in via ssh, execute the command 'dpkg' and get version.

Vulnerability Detection Result

```
Detected GNU Binutils
Version: 2.24
Location: /
CPE: cpe:/a:gnu:binutils:2.24
Concluded from version identification result:
2.24
```

Log Method

Details:`GNU Binutils Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806085
Version used: `$Revision: 1970 $`

Log (CVSS: 0.0)
NVT: libpng Version Detection

Summary

Detection of installed version of libpng.
The script logs in via ssh, searches for executable 'libpng-config' and queries the found executables via command line option '-v'.

Vulnerability Detection Result

```
Detected libpng version: 1.2.50
Location: /usr/bin/libpng-config
CPE: cpe:/a:libpng:libpng:1.2.50
Concluded from version identification result:
1.2.50
```

Log Method

Details:`libpng Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900070
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: OpenJDK Version Detection

Summary

This script detects the installed version of OpenJDK and sets the reuslt in KB.

Vulnerability Detection Result

```
Detected OpenJDK version: 2.5.6.0
Location: /usr/bin/java
CPE: cpe:/a:sun:openjdk:2.5.6.0
```

... continues on next page ...

. . . continued from previous page . . .

```
Concluded from version identification result:
java version "1.7.0_79"
OpenJDK Runtime Environment (IcedTea 2.5.6) (7u79-2.5.6-0ubuntu1.14.04.1)
OpenJDK 64-Bit Server VM (build 24.79-b02, mixed mode)
```

Log Method
Details:`OpenJDK Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900334
Version used: `$Revision: 15 $`

Log (CVSS: 0.0)
NVT: Avahi Version Detection (Linux)

Summary
Detection of installed version of Avahi Daemon.
The script logs in via ssh, searches for executable 'avahi-daemon' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected Avahi version: 0.6.31
Location: /usr/sbin/avahi-daemon
CPE: cpe:/a:avahi:avahi:0.6.31
Concluded from version identification result:
avahi-daemon 0.6.31
```

Log Method
Details:`Avahi Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900416
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: HP Linux Imaging and Printing System Version Detection (Linux)

Summary
Detection of installed version of HP Linux Imaging and Printing System.
The script logs in via ssh, searches for executable 'avahi-daemon' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected HP Linux Imaging and Printing System version: 3.14.3
Location: /usr/bin/hp-setup
CPE: cpe:/a:hp:hplip:3.14.3
Concluded from version identification result:
 [01mHP Linux Imaging and Printing System (ver. 3.14.3) [0m
 [01mPrinter/Fax Setup Utility ver. 9.0 [0m
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Copyright (c) 2001-13 Hewlett-Packard Development Company, LP
This software comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to distribute it
under certain conditions. See COPYING file for more details.
Installs HPLIP printers and faxes in the CUPS spooler. Tries to automatically de
↪termine the correct PPD file to use. Allows the printing of a testpage. Perfor
↪ms basic fax parameter setup.
 [01mUsage: hp-setup [MODE] [OPTIONS] [SERIAL NO.|USB bus:device|IP|DEVNODE] [0m
 [01m[MODE] [0m
  Run in graphical    -u or --gui (Default)
  UI mode:
  Run in interactive  -i or --interactive
  mode:
 [01m[OPTIONS] [0m
  Automatic mode:     -a or --auto (-i mode only)
  To specify the      --port=<port> (Valid values are 1*, 2, and 3.
  port on a           *default)
  multi-port
  JetDirect:
  No testpage in      -x (-i mode only)
  automatic mode:
  To specify a CUPS   -p<printer> or --printer=<printer> (-i mode only)
  printer queue
  name:
  To specify a CUPS   -f<fax> or --fax=<fax> (-i mode only)
  fax queue name:
  Type of queue(s)    -t<typelist> or --type=<typelist>. <typelist>: print*,
  to install:         fax* (*default) (-i mode only)
  To specify the      -d<device> or --device=<device> (--qt4 mode only)
  device URI to
  install:
  Remove printers or  -r or --rm or --remove
  faxes instead of
  setting-up:
  Set the language:   -q <lang> or --lang=<lang>. Use -q? or --lang=? to see
                      a list of available language codes.
  Set the logging     -l<level> or --logging=<level>
  level:
                      <level>: none, info*, error, warn, debug (*default)
  Run in debug mode:  -g (same as option: -ldebug)
  This help           -h or --help
  information:
 [01m[SERIAL NO.|USB ID|IP|DEVNODE] [0m
  USB bus:device      "xxx:yyy" where 'xxx' is the USB bus and 'yyy' is the
  (usb only):         USB device. (Note: The ':' and all leading zeros must
                      be present.)
                      Use the 'lsusb' command to obtain this information.
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  IPs (network        IPv4 address "a.b.c.d" or "hostname"
  only):
  DEVNODE (parallel   "/dev/parportX", X=0,1,2,...
  only):
  SERIAL NO. (usb     "serial no."
  and parallel
  only):
 [01mExamples: [0m
  Setup using GUI     $ hp-setup
  mode:
  Setup using GUI     $ hp-setup -b usb
  mode, specifying
  usb:
  Setup using GUI     $ hp-setup 192.168.0.101
  mode, specifying
  an IP:
  One USB printer     $ hp-setup -i -a
  attached,
  automatic:
  USB, IDs            $ hp-setup -i 001:002
  specified:
  Network:            $ hp-setup -i 66.35.250.209
  Network, Jetdirect  $ hp-setup -i --port=2 66.35.250.209
  port 2:
  Parallel:           $ hp-setup -i /dev/parport0
  USB or parallel,    $ hp-setup -i US12345678A
  using serial
  number:
  USB, automatic:     $ hp-setup -i --auto 001:002
  Parallel,           $ hp-setup -i -a -x /dev/parport0
  automatic, no
  testpage:
  Parallel, choose    $ hp-setup -i -b par
  device:
 [01mNotes: [0m
1. If no serial number, USB ID, IP, or device node is specified, the USB and par
↪allel busses will be probed for devices.
2. Using 'lsusb' to obtain USB IDs: (example)
 $ lsusb
 Bus 003 Device 011: ID 03f0:c202 Hewlett-Packard
 $ hp-setup --auto 003:011
 (Note: You may have to run 'lsusb' from /sbin or another location. Use '$ locat
↪e lsusb' to determine this.)
3. Parameters -a, -f, -p, or -t are not valid in GUI (-u) mode.
 [01mSee Also: [0m
hp-makeuri
hp-probe
```

. . . continues on next page . . .

. . . continued from previous page . . .

Log Method
Details:`HP Linux Imaging and Printing System Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900428
Version used: `$Revision: 1128 $`

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

Summary
Detection of installed version of VLC Media Player version on Linux.
This script logs in via shh, extracts the version from the binary file and set it in KB.

Vulnerability Detection Result

```
Detected VLC Media Player
Version: 2.1.6
Location: /usr/bin/vlc
CPE: cpe:/a:videolan:vlc_media_player:2.1.6
Concluded from version identification result:
2.1.6
```

Log Method
Details:`VLC Media Player Version Detection (Lin)`
OID:1.3.6.1.4.1.25623.1.0.900529
Version used: `$Revision: 907 $`

Log (CVSS: 0.0)
NVT: Ghostscript Version Detection (Linux)

Summary
Detection of installed version of Ghostscript.
The script logs in via ssh, searches for executable 'gs' and queries the found executables via command line option '–help'.

Vulnerability Detection Result

```
Detected Ghostscript version: 9.10
Location: /usr/bin/gs
CPE: cpe:/a:ghostscript:ghostscript:9.10
Concluded from version identification result:
9.10
```

Log Method
Details:`Ghostscript Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900541
Version used: `$Revision: 1040 $`

Log (CVSS: 0.0)
NVT: ImageMagick version Detection (Linux)

Summary

Detection of installed version of ImageMagick.
The script logs in via ssh, searches for executable 'identify' and queries the found executables via command line option '-version'.

Vulnerability Detection Result

```
Detected ImageMagick version: 6.7.7.1
Location: /usr/bin/identify
CPE: cpe:/a:imagemagick:imagemagick:6.7.7.1
Concluded from version identification result:
Version: ImageMagick 6.7.7-10 2014-03-06 Q16 http://www.imagemagick.org
Copyright: Copyright (C) 1999-2012 ImageMagick Studio LLC
Features: OpenMP
```

Log Method

Details:`ImageMagick version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900563
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: Ruby Version Detection (Linux)

Summary

Detection of installed version of Ruby.
The script logs in via ssh, searches for executable 'ruby' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected Ruby version: 1.9.3.p484
Location: /usr/bin/ruby
CPE: cpe:/a:ruby-lang:ruby:1.9.3.p484:p484
Concluded from version identification result:
ruby 1.9.3p484 (2013-11-22 revision 43786) [x86_64-linux]
```

Log Method

Details:`Ruby Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900569
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: ISC DHCP Client Version Detection

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Detection of installed version of ISC DHCP Client.
The script logs in via ssh, searches for executable 'dhclient' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected ISC DHCP Client version: 4.2.4
Location: /sbin/dhclient
CPE: cpe:/a:isc:dhcp:4.2.4
Concluded from version identification result:
isc-dhclient-4.2.4
```

Log Method

Details:`ISC DHCP Client Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900696
Version used: `$Revision: 1128 $`

Log (CVSS: 0.0)
NVT: LibreOffice Version Detection (Linux)

Summary

This script finds the installed LibreOffice version and saves the result in KB.

Vulnerability Detection Result

```
LibreOffice version 4.2.8.2.2 running at location /usr/bin/libreoffice
 was detected on the host
```

Log Method

Details:`LibreOffice Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.902701
Version used: `$Revision: 1040 $`

[return to 192.168.1.10]