Scan Report

December 17, 2020

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 “metasplunk”. The scan started at Thu Dec 17 10:59:16 2020 UTC and ended at Thu Dec 17 11:03:16 2020 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
10.0.3.5	37	63	6	0	0
Total: 1	37	63	6	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level “Log” are not shown.
Issues with the threat level “Debug” are not shown.
Issues with the threat level “False Positive” are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 106 results selected by the filtering described above. Before filtering there were 508 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.0.3.5	SSH	Success	Protocol SSH, Port 22, User msfadmin

2 Results per Host

2.1 10.0.3.5

Host scan start Thu Dec 17 10:59:57 2020 UTC
Host scan end Thu Dec 17 11:03:13 2020 UTC

Service (Port)	Threat Level
general/tcp	High
general/tcp	Medium
general/tcp	Low

2.1.1 High general/tcp

High (CVSS: 10.0) NVT: GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 04

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:gnu:bash:3.2.33
Detected by GNU Bash Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.10825
↪8)
```

Summary

This host is installed with GNU Bash Shell and is prone to remote command execution vulnerability.

Vulnerability Detection Result

```
Used command: echo "vt_test='() { x() { _;}; x() { _;} <<a; }' /bin/bash -c date
↪ 2>/dev/null || echo CVE-2014-6277 vulnerable" | /bin/bash
Result: /bin/bash: line 1:  6514 Segmentation fault      vt_test='() { x() { _;}
↪; x() { _;} <<a; }' /bin/bash -c date 2> /dev/null
CVE-2014-6277 vulnerable
```

Impact

Successful exploitation will allow remote or local attackers to inject shell commands, allowing local privilege escalation or remote command execution depending on the application vector.

Solution

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

GNU Bash through 4.3 bash43-026.

Vulnerability Insight

GNU bash contains a flaw that is triggered when evaluating environment variables passed from another environment. After processing a function definition, bash continues to process trailing strings. Incomplete fix to CVE-2014-7169, CVE-2014-6271.

Vulnerability Detection Method

Login to the target machine with ssh credentials and check its possible to execute the commands via GNU bash shell.

Details: `GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 04`

OID:1.3.6.1.4.1.25623.1.0.802086

Version used: `2020-08-24T11:37:53Z`

Product Detection Result

Product: `cpe:/a:gnu:bash:3.2.33`

Method: `GNU Bash Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.108258)

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2014-6277
bid: 70165
url: https://shellshocker.net
url: http://lcamtuf.blogspot.in/2014/09/bash-bug-apply-unofficial-patch-now.html
cert-bund: CB-K17/1709
cert-bund: CB-K16/1819
cert-bund: CB-K15/1437
cert-bund: CB-K15/0118
cert-bund: CB-K14/1196
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2016-1928
dfn-cert: DFN-CERT-2015-1514
dfn-cert: DFN-CERT-2014-1258
```

High (CVSS: 10.0)
NVT: Ubuntu Update for apt USN-1215-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1215-1

Vulnerability Detection Result

```
Vulnerable package: apt
Installed version:  0.7.9ubuntu17
Fixed version:      0.7.9ubuntu17.3
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
apt on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that the apt-key utility incorrectly verified GPG keys when downloaded via the net-update option. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to install altered packages. This update corrects the issue by disabling the net-update option completely. A future update will re-enable the option with corrected verification.

Vulnerability Detection Method
Details: `Ubuntu Update for apt USN-1215-1`
OID:1.3.6.1.4.1.25623.1.0.840752
Version used: `2019-03-13T09:25:59Z`

References

```
url: http://www.ubuntu.com/usn/usn-1215-1/
usn: 1215-1
```

High (CVSS: 10.0)
NVT: Ubuntu Update for samba USN-1423-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1423-1

Vulnerability Detection Result

```
Vulnerable package: samba
Installed version:  3.0.20-0.1ubuntu1
Fixed version:      3.0.28a-1ubuntu4.18
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
samba on Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Brian Gorenc discovered that Samba incorrectly calculated array bounds when handling remote procedure calls (RPC) over the network. A remote, unauthenticated attacker could exploit this to execute arbitrary code as the root user. (CVE-2012-1182)

Vulnerability Detection Method
Details: `Ubuntu Update for samba USN-1423-1`
OID:1.3.6.1.4.1.25623.1.0.840980
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-1182
url: http://www.ubuntu.com/usn/usn-1423-1/
usn: 1423-1
dfn-cert: DFN-CERT-2013-0359
dfn-cert: DFN-CERT-2013-0351
dfn-cert: DFN-CERT-2012-1172
dfn-cert: DFN-CERT-2012-1111
dfn-cert: DFN-CERT-2012-0986
dfn-cert: DFN-CERT-2012-0950
dfn-cert: DFN-CERT-2012-0929
dfn-cert: DFN-CERT-2012-0850
dfn-cert: DFN-CERT-2012-0764
dfn-cert: DFN-CERT-2012-0748
dfn-cert: DFN-CERT-2012-0730
dfn-cert: DFN-CERT-2012-0727
dfn-cert: DFN-CERT-2012-0726
dfn-cert: DFN-CERT-2012-0721
dfn-cert: DFN-CERT-2012-0720
dfn-cert: DFN-CERT-2012-0719
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0718
dfn-cert: DFN-CERT-2012-0713
dfn-cert: DFN-CERT-2012-0666
dfn-cert: DFN-CERT-2012-0665
dfn-cert: DFN-CERT-2012-0657
```

High (CVSS: 10.0)
NVT: GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC)

Product detection result

```
cpe:/a:gnu:bash:3.2.33
Detected by GNU Bash Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.10825
↪8)
```

Summary

This host is installed with GNU Bash Shell and is prone to remote command execution vulnerability.

Vulnerability Detection Result

```
Used command: echo 'env x="() { :;}; echo CVE-2014-6271 vulnerable" /bin/bash -c
↪ "echo this is a test"' | /bin/bash
Result: CVE-2014-6271 vulnerable
this is a test
```

Impact

Successful exploitation will allow remote or local attackers to inject shell commands, allowing local privilege escalation or remote command execution depending on the application vector.

Solution

Solution type: VendorFix

Apply the patch or upgrade to latest version.

Affected Software/OS

GNU Bash through 4.3.

Vulnerability Insight

GNU bash contains a flaw that is triggered when evaluating environment variables passed from another environment. After processing a function definition, bash continues to process trailing strings.

Vulnerability Detection Method

Login to the target machine with ssh credentials and check its possible to execute the commands via GNU bash shell.

Details: `GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC)`

OID:1.3.6.1.4.1.25623.1.0.804490

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2020-08-24T11:37:53Z

Product Detection Result

Product: cpe:/a:gnu:bash:3.2.33
Method: GNU Bash Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.108258)

References

```
cve: CVE-2014-6271
bid: 70103
url: https://access.redhat.com/solutions/1207723
url: https://bugzilla.redhat.com/show_bug.cgi?id=1141597
url: https://blogs.akamai.com/2014/09/environment-bashing.html
url: https://community.qualys.com/blogs/securitylabs/2014/09/24/
cert-bund: CB-K17/1709
cert-bund: CB-K14/1313
cert-bund: CB-K14/1245
cert-bund: CB-K14/1199
cert-bund: CB-K14/1196
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2014-1307
dfn-cert: DFN-CERT-2014-1261
dfn-cert: DFN-CERT-2014-1258
```

High (CVSS: 10.0)
NVT: GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 03

Product detection result

```
cpe:/a:gnu:bash:3.2.33
Detected by GNU Bash Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.10825
↪8)
```

Summary

This host is installed with GNU Bash Shell and is prone to remote command execution vulnerability.

Vulnerability Detection Result

```
Used command: echo "vt_test='() { echo CVE-2014-6278 vulnerable; }' /bin/bash -c
↪ vt_test" | /bin/bash
Result: CVE-2014-6278 vulnerable
```

Impact

Successful exploitation will allow remote or local attackers to inject shell commands, allowing local privilege escalation or remote command execution depending on the application vector.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
GNU Bash through 4.3 bash43-026.

Vulnerability Insight
GNU bash contains a flaw that is triggered when evaluating environment variables passed from another environment. After processing a function definition, bash continues to process trailing strings. Incomplete fix to CVE-2014-7169, CVE-2014-6271, and CVE-2014-6277.

Vulnerability Detection Method
Login to the target machine with ssh credentials and check its possible to execute the commands via GNU bash shell.
Details: GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 03
OID:1.3.6.1.4.1.25623.1.0.802085
Version used: 2020-08-24T11:37:53Z

Product Detection Result
Product: cpe:/a:gnu:bash:3.2.33
Method: GNU Bash Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.108258)

References
cve: CVE-2014-6278
bid: 70166
url: https://shellshocker.net/
url: http://lcamtuf.blogspot.in/2014/09/bash-bug-apply-unofficial-patch-now.html
cert-bund: CB-K17/1709
cert-bund: CB-K16/1819
cert-bund: CB-K14/1196
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2016-1928
dfn-cert: DFN-CERT-2014-1258

High (CVSS: 10.0)
NVT: GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 02

Product detection result
cpe:/a:gnu:bash:3.2.33
Detected by GNU Bash Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.10825
↪8)

. . . continues on next page . . .

... continued from previous page ...

Summary

This host is installed with GNU Bash Shell and is prone to remote command execution vulnerability.

Vulnerability Detection Result

```
Used command: echo "cd /tmp; rm -f /tmp/echo; env X='() { (VT Test)=>\' /bin/bas
↪h -c 'echo id'; cat echo; rm -f /tmp/echo" | /bin/bash
Result: /bin/bash: X: line 1: syntax error near unexpected token `='
/bin/bash: X: line 1: `'
/bin/bash: error importing function definition for `X'
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(flo
↪ppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin)
↪,119(sambashare),1000(msfadmin)
```

Impact

Successful exploitation will allow remote or local attackers to inject shell commands, allowing local privilege escalation or remote command execution depending on the application vector.

Solution

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

GNU Bash through 4.3 bash43-025.

Vulnerability Insight

GNU bash contains a flaw that is triggered when evaluating environment variables passed from another environment. After processing a function definition, bash continues to process trailing strings. Incomplete fix to CVE-2014-6271.

Vulnerability Detection Method

Login to the target machine with ssh credentials and check its possible to execute the commands via GNU bash shell.

Details: `GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 02`

OID:1.3.6.1.4.1.25623.1.0.802082

Version used: `2020-08-24T11:37:53Z`

Product Detection Result

Product: `cpe:/a:gnu:bash:3.2.33`

Method: `GNU Bash Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.108258)

References

```
cve: CVE-2014-7169
bid: 70137
```

... continues on next page ...

. . . continued from previous page . . .

```
url: https://shellshocker.net/
url: http://www.kb.cert.org/vuls/id/252743
url: http://www.openwall.com/lists/oss-security/2014/09/24/32
url: https://community.qualys.com/blogs/securitylabs/2014/09/24/bash-remote-code
↪-execution-vulnerability-cve-2014-6271
cert-bund: CB-K17/1709
cert-bund: CB-K14/1313
cert-bund: CB-K14/1245
cert-bund: CB-K14/1196
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2014-1307
dfn-cert: DFN-CERT-2014-1258
```

High (CVSS: 10.0)
NVT: OS End Of Life Detection

Product detection result

```
cpe:/o:canonical:ubuntu_linux:8.04:-:lts
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)
```

Summary

OS End Of Life Detection.
The Operating System on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

```
The "Ubuntu" Operating System on the remote host has reached the end of life.
CPE:                cpe:/o:canonical:ubuntu_linux:8.04:-:lts
Installed version,
build or SP:        8.04
EOL date:           2013-05-09
EOL info:           https://wiki.ubuntu.com/Releases
```

Solution

Solution type: Mitigation
Upgrade the Operating System on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerability Detection Method

Details: `OS End Of Life Detection`
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: `2020-08-25T06:34:32Z`

Product Detection Result

Product: `cpe:/o:canonical:ubuntu_linux:8.04:-:lts`

. . . continues on next page . . .

. . . continued from previous page . . .

Method: `OS Detection Consolidation and Reporting`
OID: 1.3.6.1.4.1.25623.1.0.105937)

High (CVSS: 10.0)
NVT: Ubuntu Update for freetype USN-1403-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1403-1

Vulnerability Detection Result

```
Vulnerable package: libfreetype6
Installed version:  2.3.5-1ubuntu4.8.04.2
Fixed version:      2.3.5-1ubuntu4.8.04.9
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
freetype on Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed BDF font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash. (CVE-2012-1126)
Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed BDF font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash. (CVE-2012-1127)
Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed TrueType font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash. (CVE-2012-1128)
Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed Type42 font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash. (CVE-2012-1129)
Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed PCF font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash. (CVE-2012-1130)
Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed TrueType font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash. (CVE-2012-1131)
Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed Type1 font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash. (CVE-2012-1132)
Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed BDF font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges. (CVE-2012-1133)

. . . continues on next page . . .

. . . continued from previous page . . .

Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed Type1 font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges. (CVE-2012-1134)
Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed TrueType font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash. (CVE-2012-1135)
Mateusz Jurczyk discovere ...
Description truncated, please see the referenced URL(s) for more information.

Vulnerability Detection Method
Details: `Ubuntu Update for freetype USN-1403-1`
OID:1.3.6.1.4.1.25623.1.0.840959
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-1126
cve: CVE-2012-1127
cve: CVE-2012-1128
cve: CVE-2012-1129
cve: CVE-2012-1130
cve: CVE-2012-1131
cve: CVE-2012-1132
cve: CVE-2012-1133
cve: CVE-2012-1134
cve: CVE-2012-1135
cve: CVE-2012-1136
cve: CVE-2012-1137
cve: CVE-2012-1138
cve: CVE-2012-1139
cve: CVE-2012-1140
cve: CVE-2012-1141
cve: CVE-2012-1142
cve: CVE-2012-1143
cve: CVE-2012-1144
url: http://www.ubuntu.com/usn/usn-1403-1/
usn: 1403-1
dfn-cert: DFN-CERT-2013-0178
dfn-cert: DFN-CERT-2012-1248
dfn-cert: DFN-CERT-2012-1185
dfn-cert: DFN-CERT-2012-0820
dfn-cert: DFN-CERT-2012-0814
dfn-cert: DFN-CERT-2012-0791
dfn-cert: DFN-CERT-2012-0777
dfn-cert: DFN-CERT-2012-0753
dfn-cert: DFN-CERT-2012-0752
dfn-cert: DFN-CERT-2012-0711
dfn-cert: DFN-CERT-2012-0709
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0705
dfn-cert: DFN-CERT-2012-0700
dfn-cert: DFN-CERT-2012-0698
dfn-cert: DFN-CERT-2012-0660
dfn-cert: DFN-CERT-2012-0450
```

High (CVSS: 10.0)
NVT: Pidgin MSN SLP Packets Denial Of Service Vulnerability (Linux)

Product detection result

```
cpe:/a:pidgin:pidgin:2.5.2
Detected by Pidgin Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.900661)
```

Summary

This host has Pidgin installed and is prone to Denial of Service vulnerability.

Vulnerability Detection Result

```
Installed version: 2.5.2
Fixed version:     2.5.9
```

Impact

Attackers can exploit this issue to execute arbitrary code, corrupt memory and cause the application to crash.

Solution

Solution type: VendorFix

Upgrade to Pidgin version 2.5.9.

Affected Software/OS

Pidgin version prior to 2.5.9 on Linux.

Vulnerability Insight

An error in the 'msn_slplink_process_msg()' function while processing malformed MSN SLP packets which can be exploited to overwrite an arbitrary memory location.

Vulnerability Detection Method

Details: `Pidgin MSN SLP Packets Denial Of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900920
Version used: `2018-12-05T14:14:20Z`

Product Detection Result

Product: `cpe:/a:pidgin:pidgin:2.5.2`
Method: `Pidgin Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.900661)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2009-2694
bid: 36071
url: http://secunia.com/advisories/36384
url: http://www.pidgin.im/news/security/?id=34
url: http://www.vupen.com/english/advisories/2009/2303
dfn-cert: DFN-CERT-2009-1707
dfn-cert: DFN-CERT-2009-1292
dfn-cert: DFN-CERT-2009-1283
dfn-cert: DFN-CERT-2009-1191
dfn-cert: DFN-CERT-2009-1173
dfn-cert: DFN-CERT-2009-1164
dfn-cert: DFN-CERT-2009-1154
```

High (CVSS: 10.0)
NVT: GNU Bash Stacked Redirects aka 'redir_stack' Memory Corruption Vulnerability (LSC)

Product detection result

```
cpe:/a:gnu:bash:3.2.33
Detected by GNU Bash Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.10825
↪8)
```

Summary

This host is installed with GNU Bash Shell and is prone to command execution vulnerability.

Vulnerability Detection Result

```
Used command: /bin/bash -c 'true <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF
↪ <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF' || echo 'CVE-2014-7186 vulnerable, redir
↪_stack'
Result: bash: line 1:  6546 Segmentation fault      /bin/bash -c 'true <<EOF <<E
↪OF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF'
CVE-2014-7186 vulnerable, redir_stack
```

Impact

Successful exploitation will allow attackers to corrupt memory to cause a crash or potentially execute arbitrary coommands.

Solution

Solution type: VendorFix

Apply the appropriate patch.

Affected Software/OS

GNU Bash through 4.3 bash43-026.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

GNU bash contains a flaw that is triggered when evaluating untrusted input during stacked redirects handling.

Vulnerability Detection Method

Login to the target machine with ssh credentials and check its possible to execute the commands via GNU bash shell.

Details: `GNU Bash Stacked Redirects aka 'redir_stack' Memory Corruption Vulnerability (L.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.802083

Version used: `2020-08-24T11:37:53Z`

Product Detection Result

Product: `cpe:/a:gnu:bash:3.2.33`

Method: `GNU Bash Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.108258)

References

```
cve: CVE-2014-7186
bid: 70152
url: https://shellshocker.net/
url: http://openwall.com/lists/oss-security/2014/09/26/2
url: http://openwall.com/lists/oss-security/2014/09/25/32
url: http://lcamtuf.blogspot.in/2014/09/bash-bug-apply-unofficial-patch-now.html
cert-bund: CB-K15/1437
cert-bund: CB-K15/0118
cert-bund: CB-K14/1245
cert-bund: CB-K14/1196
dfn-cert: DFN-CERT-2015-1514
dfn-cert: DFN-CERT-2014-1307
dfn-cert: DFN-CERT-2014-1258
```

High (CVSS: 9.3)
NVT: Ubuntu Update for libxml2 USN-1334-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1334-1

Vulnerability Detection Result

```
Vulnerable package: libxml2
Installed version:  2.6.31.dfsg-2ubuntu1
Fixed version:      2.6.31.dfsg-2ubuntu1.7
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
libxml2 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that libxml2 contained an off by one error. If a user or application linked against libxml2 were tricked into opening a specially crafted XML file, an attacker could cause the application to crash or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-0216)
It was discovered that libxml2 is vulnerable to double-free conditions when parsing certain XML documents. This could allow a remote attacker to cause a denial of service. (CVE-2011-2821, CVE-2011-2834)
It was discovered that libxml2 did not properly detect end of file when parsing certain XML documents. An attacker could exploit this to crash applications linked against libxml2. (CVE-2011-3905)
It was discovered that libxml2 did not properly decode entity references with long names. If a user or application linked against libxml2 were tricked into opening a specially crafted XML file, an attacker could cause the application to crash or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-3919)

Vulnerability Detection Method
Details: `Ubuntu Update for libxml2 USN-1334-1`
OID:1.3.6.1.4.1.25623.1.0.840868
Version used: `2019-03-13T09:25:59Z`

References
```
cve: CVE-2011-0216
cve: CVE-2011-2821
cve: CVE-2011-2834
cve: CVE-2011-3905
cve: CVE-2011-3919
url: http://www.ubuntu.com/usn/usn-1334-1/
usn: 1334-1
dfn-cert: DFN-CERT-2013-0196
dfn-cert: DFN-CERT-2012-1873
dfn-cert: DFN-CERT-2012-1361
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1191
dfn-cert: DFN-CERT-2012-0812
dfn-cert: DFN-CERT-2012-0215
dfn-cert: DFN-CERT-2012-0208
dfn-cert: DFN-CERT-2012-0152
dfn-cert: DFN-CERT-2012-0139
dfn-cert: DFN-CERT-2012-0107
dfn-cert: DFN-CERT-2012-0082
dfn-cert: DFN-CERT-2012-0072
dfn-cert: DFN-CERT-2012-0067
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0066
dfn-cert: DFN-CERT-2012-0065
dfn-cert: DFN-CERT-2011-1927
dfn-cert: DFN-CERT-2011-1854
dfn-cert: DFN-CERT-2011-1573
```

High (CVSS: 9.3)
NVT: Ubuntu Update for freetype USN-1267-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1267-1

Vulnerability Detection Result

```
Vulnerable package: libfreetype6
Installed version:  2.3.5-1ubuntu4.8.04.2
Fixed version:      2.3.5-1ubuntu4.8.04.7
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
freetype on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that FreeType did not correctly handle certain malformed Type 1 font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges. (CVE-2011-3256)
It was discovered that FreeType did not correctly handle certain malformed CID-keyed PostScript font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges. (CVE-2011-3439)

Vulnerability Detection Method
Details: `Ubuntu Update for freetype USN-1267-1`
OID:1.3.6.1.4.1.25623.1.0.840810
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-3256
cve: CVE-2011-3439
url: http://www.ubuntu.com/usn/usn-1267-1/
usn: 1267-1
dfn-cert: DFN-CERT-2012-0777
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0190
dfn-cert: DFN-CERT-2012-0020
dfn-cert: DFN-CERT-2011-1868
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-1867
dfn-cert: DFN-CERT-2011-1835
dfn-cert: DFN-CERT-2011-1815
dfn-cert: DFN-CERT-2011-1793
dfn-cert: DFN-CERT-2011-1792
dfn-cert: DFN-CERT-2011-1781
dfn-cert: DFN-CERT-2011-1767
dfn-cert: DFN-CERT-2011-1735
dfn-cert: DFN-CERT-2011-1650
dfn-cert: DFN-CERT-2011-1645
dfn-cert: DFN-CERT-2011-1638
```

High (CVSS: 9.3)
NVT: Ubuntu Update for libxml2 USN-1153-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1153-1

Vulnerability Detection Result

```
Vulnerable package: libxml2
Installed version:  2.6.31.dfsg-2ubuntu1
Fixed version:      2.6.31.dfsg-2ubuntu1.6
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
libxml2 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Chris Evans discovered that libxml2 incorrectly handled memory allocation. If an application using libxml2 opened a specially crafted XML file, an attacker could cause a denial of service or possibly execute code as the user invoking the program.

Vulnerability Detection Method
Details: `Ubuntu Update for libxml2 USN-1153-1`
OID:1.3.6.1.4.1.25623.1.0.840679
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-1944
url: http://www.ubuntu.com/usn/usn-1153-1/
usn: 1153-1
cert-bund: CB-K15/0079
cert-bund: CB-K15/0050
dfn-cert: DFN-CERT-2015-0079
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0049
dfn-cert: DFN-CERT-2013-0196
dfn-cert: DFN-CERT-2012-1873
dfn-cert: DFN-CERT-2012-1361
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1191
dfn-cert: DFN-CERT-2012-0812
dfn-cert: DFN-CERT-2012-0208
dfn-cert: DFN-CERT-2012-0066
dfn-cert: DFN-CERT-2011-1854
dfn-cert: DFN-CERT-2011-1563
dfn-cert: DFN-CERT-2011-1340
dfn-cert: DFN-CERT-2011-1015
```

High (CVSS: 9.3)
NVT: Ubuntu Update for tiff vulnerabilities USN-1085-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1085-1

Vulnerability Detection Result

```
Vulnerable package: libtiff4
Installed version:  3.8.2-7ubuntu3.4
Fixed version:      3.8.2-7ubuntu3.7
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
tiff vulnerabilities on Ubuntu 6.06 LTS, Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight
Sauli Pahlman discovered that the TIFF library incorrectly handled invalid td_stripbytecount fields. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2010-2482)
Sauli Pahlman discovered that the TIFF library incorrectly handled TIFF files with an invalid combination of SamplesPerPixel and Photometric values. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service. This issue only affected Ubuntu 10.10. (CVE-2010-2482)
Nicolae Ghimbovschi discovered that the TIFF library incorrectly handled invalid ReferenceBlackWhite values. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service. (CVE-2010-2595)

. . . continues on next page . . .

... continued from previous page ...

Sauli Pahlman discovered that the TIFF library incorrectly handled certain default fields. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service. (CVE-2010-2597, CVE-2010-2598)

It was discovered that the TIFF library incorrectly validated certain data types. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service. (CVE-2010-2630)

It was discovered that the TIFF library incorrectly handled downsampled JPEG data. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could execute arbitrary code with user privileges, or crash the application, leading to a denial of service. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2010-3087)

It was discovered that the TIFF library incorrectly handled certain JPEG data. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could execute arbitrary code with user privileges, or crash the application, leading to a denial of service. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS and 9.10. (CVE-2011-0191)

It was discovered that the TIFF library incorrectly handled certain TIFF FAX images. If a user or automated system were tricked into opening a specially crafted TIFF FAX image, a remote attacker could execute arbitrary code with user privileges, or crash the application, leading to a denial of service. (CVE-2011-0191)

Vulnerability Detection Method

Details: `Ubuntu Update for tiff vulnerabilities USN-1085-1`
OID:1.3.6.1.4.1.25623.1.0.840610
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2010-2482
cve: CVE-2010-2483
cve: CVE-2010-2595
cve: CVE-2010-2597
cve: CVE-2010-2598
cve: CVE-2010-2630
cve: CVE-2010-3087
cve: CVE-2011-0191
cve: CVE-2011-0192
url: http://www.ubuntu.com/usn/usn-1085-1/
usn: 1085-1
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2012-1879
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2011-1002
dfn-cert: DFN-CERT-2011-1001
dfn-cert: DFN-CERT-2011-0803
dfn-cert: DFN-CERT-2011-0771
dfn-cert: DFN-CERT-2011-0695
dfn-cert: DFN-CERT-2011-0681
dfn-cert: DFN-CERT-2011-0667
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-0541
dfn-cert: DFN-CERT-2011-0537
dfn-cert: DFN-CERT-2011-0503
dfn-cert: DFN-CERT-2011-0493
dfn-cert: DFN-CERT-2011-0492
dfn-cert: DFN-CERT-2011-0455
dfn-cert: DFN-CERT-2011-0360
dfn-cert: DFN-CERT-2011-0329
dfn-cert: DFN-CERT-2011-0317
dfn-cert: DFN-CERT-2011-0291
dfn-cert: DFN-CERT-2010-1295
dfn-cert: DFN-CERT-2010-1247
dfn-cert: DFN-CERT-2010-1005
dfn-cert: DFN-CERT-2010-1004
dfn-cert: DFN-CERT-2010-0876
dfn-cert: DFN-CERT-2010-0873
```

High (CVSS: 9.3)
NVT: Ubuntu Update for openssl USN-1357-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1357-1

Vulnerability Detection Result

```
Vulnerable package: openssl
Installed version:  0.9.8g-4ubuntu3
Fixed version:      0.9.8g-4ubuntu3.15
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
openssl on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that the elliptic curve cryptography (ECC) subsystem in OpenSSL, when using the Elliptic Curve Digital Signature Algorithm (ECDSA) for the ECDHE_ECDSA cipher suite, did not properly implement curves over binary fields. This could allow an attacker to determine private keys via a timing attack. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-1945)
Adam Langley discovered that the ephemeral Elliptic Curve Diffie-Hellman (ECDH) functionality in OpenSSL did not ensure thread safety while processing handshake messages from clients. This could allow a remote attacker to cause a denial of service via out-of-order messages that violate the TLS protocol. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-3210)

. . . continues on next page . . .

... continued from previous page ...

Nadhem Alfardan and Kenny Paterson discovered that the Datagram Transport Layer Security (DTLS) implementation in OpenSSL performed a MAC check only if certain padding is valid. This could allow a remote attacker to recover plaintext. (CVE-2011-4108)

Antonio Martin discovered that a flaw existed in the fix to address CVE-2011-4108, the DTLS MAC check failure. This could allow a remote attacker to cause a denial of service. (CVE-2012-0050)

Ben Laurie discovered a double free vulnerability in OpenSSL that could be triggered when the X509_V_FLAG_POLICY_CHECK flag is enabled. This could allow a remote attacker to cause a denial of service. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-4109)

It was discovered that OpenSSL, in certain circumstances involving ECDH or ECDHE cipher suites, used an incorrect modular reduction algorithm in its implementation of the P-256 and P-384 NIST elliptic curves. This could allow a remote attacker to obtain the private key of a TLS server via multiple handshake attempts. This issue only affected Ubuntu 8.04 LTS. (CVE-2011-4354)

Adam Langley discovered that the SSL 3.0 implementation in OpenSSL did not properly initialize data structures for block cipher padding. This could allow a remote attacker to obtain sensitive information. (CVE-2011-4576)

Andrew Chi discovered that OpenSSL, when RFC 3779 support is enabled, could trigger an assert when handling an X.509 certificate containing certificate-extension data associated with IP address blocks or Autonomous System (AS) identifiers. This could allow a remote attacker to cause a denial of servi ...

Description truncated, please see the referenced URL(s) for more information.

Vulnerability Detection Method

Details: `Ubuntu Update for openssl USN-1357-1`

OID:1.3.6.1.4.1.25623.1.0.840887

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-1945
cve: CVE-2011-3210
cve: CVE-2011-4108
cve: CVE-2012-0050
cve: CVE-2011-4109
cve: CVE-2011-4354
cve: CVE-2011-4576
cve: CVE-2011-4577
cve: CVE-2011-4619
cve: CVE-2012-0027
url: http://www.ubuntu.com/usn/usn-1357-1/
usn: 1357-1
cert-bund: CB-K14/1017
cert-bund: CB-K14/0893
cert-bund: CB-K14/0881
cert-bund: CB-K14/0708
cert-bund: CB-K14/0262
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2014-1063
dfn-cert: DFN-CERT-2014-0924
dfn-cert: DFN-CERT-2014-0922
dfn-cert: DFN-CERT-2014-0738
dfn-cert: DFN-CERT-2014-0262
dfn-cert: DFN-CERT-2013-0391
dfn-cert: DFN-CERT-2012-1697
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1112
dfn-cert: DFN-CERT-2012-1036
dfn-cert: DFN-CERT-2012-0959
dfn-cert: DFN-CERT-2012-0859
dfn-cert: DFN-CERT-2012-0731
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0555
dfn-cert: DFN-CERT-2012-0514
dfn-cert: DFN-CERT-2012-0302
dfn-cert: DFN-CERT-2012-0183
dfn-cert: DFN-CERT-2012-0166
dfn-cert: DFN-CERT-2012-0157
dfn-cert: DFN-CERT-2012-0145
dfn-cert: DFN-CERT-2012-0137
dfn-cert: DFN-CERT-2012-0135
dfn-cert: DFN-CERT-2012-0131
dfn-cert: DFN-CERT-2012-0125
dfn-cert: DFN-CERT-2012-0117
dfn-cert: DFN-CERT-2012-0087
dfn-cert: DFN-CERT-2012-0086
dfn-cert: DFN-CERT-2012-0085
dfn-cert: DFN-CERT-2012-0084
dfn-cert: DFN-CERT-2012-0083
dfn-cert: DFN-CERT-2012-0081
dfn-cert: DFN-CERT-2012-0060
dfn-cert: DFN-CERT-2011-1490
dfn-cert: DFN-CERT-2011-1489
dfn-cert: DFN-CERT-2011-1413
```

High (CVSS: 9.3)
NVT: Ubuntu Update for tiff regression USN-1085-2

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1085-2

Vulnerability Detection Result

```
Vulnerable package: libtiff4
Installed version:  3.8.2-7ubuntu3.4
Fixed version:      3.8.2-7ubuntu3.8
```

... continues on next page ...

. . . continued from previous page . . .

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
tiff regression on Ubuntu 6.06 LTS, Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight
USN-1085-1 fixed vulnerabilities in the system TIFF library. The upstream fixes were incomplete and created problems for certain CCITTFAX4 files. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Sauli Pahlman discovered that the TIFF library incorrectly handled invalid td_stripbytecount fields. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2010-2482)
Sauli Pahlman discovered that the TIFF library incorrectly handled TIFF files with an invalid combination of SamplesPerPixel and Photometric values. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service. This issue only affected Ubuntu 10.10. (CVE-2010-2482)
Nicolae Ghimbovschi discovered that the TIFF library incorrectly handled invalid ReferenceBlackWhite values. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service. (CVE-2010-2595)
Sauli Pahlman discovered that the TIFF library incorrectly handled certain default fields. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service. (CVE-2010-2597, CVE-2010-2598)
It was discovered that the TIFF library incorrectly validated certain data types. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service. (CVE-2010-2630)
It was discovered that the TIFF library incorrectly handled downsampled JPEG data. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could execute arbitrary code with user privileges, or crash the application, leading to a denial of service. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2010-3087)
It was discovered that the TIFF library incorrectly handled certain JPEG data. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could execute arbitrary code with user privileges, or crash the application, leading to a denial of servi ...
Description truncated, please see the referenced URL(s) for more information.

Vulnerability Detection Method
Details: `Ubuntu Update for tiff regression USN-1085-2`
OID:1.3.6.1.4.1.25623.1.0.840613
Version used: `2019-03-13T09:25:59Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2010-2482
cve: CVE-2010-2595
cve: CVE-2010-2597
cve: CVE-2010-2598
cve: CVE-2010-2630
cve: CVE-2010-3087
cve: CVE-2011-0191
url: http://www.ubuntu.com/usn/usn-1085-2/
usn: 1085-2
dfn-cert: DFN-CERT-2012-1879
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2011-1002
dfn-cert: DFN-CERT-2011-1001
dfn-cert: DFN-CERT-2011-0803
dfn-cert: DFN-CERT-2011-0771
dfn-cert: DFN-CERT-2011-0695
dfn-cert: DFN-CERT-2011-0681
dfn-cert: DFN-CERT-2011-0503
dfn-cert: DFN-CERT-2011-0493
dfn-cert: DFN-CERT-2011-0492
dfn-cert: DFN-CERT-2010-1295
dfn-cert: DFN-CERT-2010-1247
dfn-cert: DFN-CERT-2010-1005
dfn-cert: DFN-CERT-2010-1004
dfn-cert: DFN-CERT-2010-0876
dfn-cert: DFN-CERT-2010-0873
```

High (CVSS: 8.5)
NVT: Ubuntu Update for mysql-5.1 USN-1397-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1397-1

Vulnerability Detection Result

```
Vulnerable package: mysql-server-5.0
Installed version:  5.0.51a-3ubuntu5
Fixed version:      5.0.95-0ubuntu1
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
mysql-5.1 on Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 5.1.61 in Ubuntu 10.04 LTS, Ubuntu 10.10, Ubuntu 11.04 and Ubuntu 11.10. Ubuntu 8.04 LTS has been updated to MySQL 5.0.95.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the references for more information.

Vulnerability Detection Method

Details: `Ubuntu Update for mysql-5.1 USN-1397-1`

OID:1.3.6.1.4.1.25623.1.0.840944

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2007-5925
cve: CVE-2008-3963
cve: CVE-2008-4098
cve: CVE-2008-4456
cve: CVE-2008-7247
cve: CVE-2009-2446
cve: CVE-2009-4019
cve: CVE-2009-4030
cve: CVE-2009-4484
cve: CVE-2010-1621
cve: CVE-2010-1626
cve: CVE-2010-1848
cve: CVE-2010-1849
cve: CVE-2010-1850
cve: CVE-2010-2008
cve: CVE-2010-3677
cve: CVE-2010-3678
cve: CVE-2010-3679
cve: CVE-2010-3680
cve: CVE-2010-3681
cve: CVE-2010-3682
cve: CVE-2010-3683
cve: CVE-2010-3833
cve: CVE-2010-3834
cve: CVE-2010-3835
cve: CVE-2010-3836
cve: CVE-2010-3837
cve: CVE-2010-3838
cve: CVE-2010-3839
cve: CVE-2010-3840
cve: CVE-2011-2262
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2012-0075
cve: CVE-2012-0087
cve: CVE-2012-0101
cve: CVE-2012-0102
cve: CVE-2012-0112
cve: CVE-2012-0113
cve: CVE-2012-0114
cve: CVE-2012-0115
cve: CVE-2012-0116
url: http://www.ubuntu.com/usn/usn-1397-1/
usn: 1397-1
url: http://dev.mysql.com/doc/refman/5.1/en/news-5-1-x.html
url: http://dev.mysql.com/doc/refman/5.0/en/news-5-0-x.html
url: http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
cert-bund: CB-K13/0919
dfn-cert: DFN-CERT-2013-1937
dfn-cert: DFN-CERT-2013-0042
dfn-cert: DFN-CERT-2012-1563
dfn-cert: DFN-CERT-2012-0936
dfn-cert: DFN-CERT-2012-0933
dfn-cert: DFN-CERT-2012-0443
dfn-cert: DFN-CERT-2012-0262
dfn-cert: DFN-CERT-2012-0249
dfn-cert: DFN-CERT-2012-0217
dfn-cert: DFN-CERT-2012-0216
dfn-cert: DFN-CERT-2012-0100
dfn-cert: DFN-CERT-2011-0079
dfn-cert: DFN-CERT-2011-0071
dfn-cert: DFN-CERT-2011-0058
dfn-cert: DFN-CERT-2010-1568
dfn-cert: DFN-CERT-2010-1524
dfn-cert: DFN-CERT-2010-1523
dfn-cert: DFN-CERT-2010-1517
dfn-cert: DFN-CERT-2010-1496
dfn-cert: DFN-CERT-2010-1491
dfn-cert: DFN-CERT-2010-1424
dfn-cert: DFN-CERT-2010-1312
dfn-cert: DFN-CERT-2010-1311
dfn-cert: DFN-CERT-2010-1078
dfn-cert: DFN-CERT-2010-0975
dfn-cert: DFN-CERT-2010-0944
dfn-cert: DFN-CERT-2010-0737
dfn-cert: DFN-CERT-2010-0736
dfn-cert: DFN-CERT-2010-0713
dfn-cert: DFN-CERT-2010-0706
dfn-cert: DFN-CERT-2010-0685
dfn-cert: DFN-CERT-2010-0655
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2010-0639
dfn-cert: DFN-CERT-2010-0638
dfn-cert: DFN-CERT-2010-0462
dfn-cert: DFN-CERT-2010-0256
dfn-cert: DFN-CERT-2010-0232
dfn-cert: DFN-CERT-2010-0214
dfn-cert: DFN-CERT-2010-0145
dfn-cert: DFN-CERT-2010-0078
dfn-cert: DFN-CERT-2009-1814
dfn-cert: DFN-CERT-2009-1769
dfn-cert: DFN-CERT-2009-1728
dfn-cert: DFN-CERT-2009-1340
dfn-cert: DFN-CERT-2009-1243
dfn-cert: DFN-CERT-2009-1235
dfn-cert: DFN-CERT-2009-1231
```

High (CVSS: 8.5)
NVT: Ubuntu Update for postgresql-9.1 USN-1789-1

Summary
The remote host is missing an update for the 'postgresql-9.1' package(s) announced via the referenced advisory.

Vulnerability Detection Result

```
Vulnerable package: postgresql-8.3
Installed version:  8.3.1-1
Fixed version:      8.3.23-0ubuntu8.04.1
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
postgresql-9.1 on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Mitsumasa Kondo and Kyotaro Horiguchi discovered that PostgreSQL incorrectly handled certain connection requests containing database names starting with a dash. A remote attacker could use this flaw to damage or destroy files within a server's data directory. This issue only applied to Ubuntu 11.10, Ubuntu 12.04 LTS, and Ubuntu 12.10. (CVE-2013-1899)
Marko Kreen discovered that PostgreSQL incorrectly generated random numbers. An authenticated attacker could use this flaw to possibly guess another database user's random numbers. (CVE-2013-1900)

. . . continues on next page . . .

. . . continued from previous page . . .

Noah Misch discovered that PostgreSQL incorrectly handled certain privilege checks. An unprivileged attacker could use this flaw to possibly interfere with in-progress backups. This issue only applied to Ubuntu 11.10, Ubuntu 12.04 LTS, and Ubuntu 12.10. (CVE-2013-1901)

Vulnerability Detection Method

Details: `Ubuntu Update for postgresql-9.1 USN-1789-1`
OID:1.3.6.1.4.1.25623.1.0.841385
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2013-1899
cve: CVE-2013-1900
cve: CVE-2013-1901
usn: 1789-1
url: http://www.ubuntu.com/usn/usn-1789-1/
cert-bund: CB-K13/0851
cert-bund: CB-K13/0666
dfn-cert: DFN-CERT-2013-1861
dfn-cert: DFN-CERT-2013-0831
dfn-cert: DFN-CERT-2013-0810
dfn-cert: DFN-CERT-2013-0741
dfn-cert: DFN-CERT-2013-0718
dfn-cert: DFN-CERT-2013-0715
dfn-cert: DFN-CERT-2013-0714
dfn-cert: DFN-CERT-2013-0713
dfn-cert: DFN-CERT-2013-0707
dfn-cert: DFN-CERT-2013-0706
dfn-cert: DFN-CERT-2013-0703
```

High (CVSS: 7.9)
NVT: Ubuntu Update for samba USN-1374-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1374-1

Vulnerability Detection Result

```
Vulnerable package: samba
Installed version:  3.0.20-0.1ubuntu1
Fixed version:      3.0.28a-1ubuntu4.17
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

samba on Ubuntu 8.04 LTS

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Andy Davis discovered that Samba incorrectly handled certain AndX offsets. A remote attacker could send a specially crafted request to the server and cause a denial of service, or possibly execute arbitrary code.

Vulnerability Detection Method

Details: `Ubuntu Update for samba USN-1374-1`
OID:1.3.6.1.4.1.25623.1.0.840908
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-0870
url: http://www.ubuntu.com/usn/usn-1374-1/
usn: 1374-1
dfn-cert: DFN-CERT-2012-0730
dfn-cert: DFN-CERT-2012-0727
dfn-cert: DFN-CERT-2012-0721
dfn-cert: DFN-CERT-2012-0462
dfn-cert: DFN-CERT-2012-0444
dfn-cert: DFN-CERT-2012-0390
dfn-cert: DFN-CERT-2012-0356
```

High (CVSS: 7.8)
NVT: Ubuntu Update for apache2 USN-1199-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1199-1

Vulnerability Detection Result

```
Vulnerable package: apache2-mpm-prefork
Installed version:  2.2.8-1ubuntu0.15
Fixed version:      2.2.8-1ubuntu0.21
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

apache2 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

A flaw was discovered in the byterange filter in Apache. A remote attacker could exploit this to cause a denial of service via resource exhaustion.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Ubuntu Update for apache2 USN-1199-1`
OID:1.3.6.1.4.1.25623.1.0.840734
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-3192
url: http://www.ubuntu.com/usn/usn-1199-1/
usn: 1199-1
dfn-cert: DFN-CERT-2012-1112
dfn-cert: DFN-CERT-2012-0856
dfn-cert: DFN-CERT-2012-0746
dfn-cert: DFN-CERT-2012-0731
dfn-cert: DFN-CERT-2011-1726
dfn-cert: DFN-CERT-2011-1725
dfn-cert: DFN-CERT-2011-1693
dfn-cert: DFN-CERT-2011-1692
dfn-cert: DFN-CERT-2011-1632
dfn-cert: DFN-CERT-2011-1631
dfn-cert: DFN-CERT-2011-1593
dfn-cert: DFN-CERT-2011-1519
dfn-cert: DFN-CERT-2011-1492
dfn-cert: DFN-CERT-2011-1440
dfn-cert: DFN-CERT-2011-1435
dfn-cert: DFN-CERT-2011-1430
dfn-cert: DFN-CERT-2011-1429
dfn-cert: DFN-CERT-2011-1425
dfn-cert: DFN-CERT-2011-1379
dfn-cert: DFN-CERT-2011-1362
dfn-cert: DFN-CERT-2011-1343
dfn-cert: DFN-CERT-2011-1342
dfn-cert: DFN-CERT-2011-1341
dfn-cert: DFN-CERT-2011-1335
dfn-cert: DFN-CERT-2011-1333
dfn-cert: DFN-CERT-2011-1318
dfn-cert: DFN-CERT-2011-1312
dfn-cert: DFN-CERT-2011-1298
```

High (CVSS: 7.8)
NVT: Ubuntu Update for bind9 USN-1601-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1601-1

Vulnerability Detection Result

```
Vulnerable package: bind9
Installed version:  9.4.2-10
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:       1:9.4.2.dfsg.P2-2ubuntu0.12
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

bind9 on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

Jake Montgomery discovered that Bind incorrectly handled certain specific combinations of RDATA. A remote attacker could use this flaw to cause Bind to crash, resulting in a denial of service.

Vulnerability Detection Method

Details: `Ubuntu Update for bind9 USN-1601-1`
OID:1.3.6.1.4.1.25623.1.0.841182
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-5166
url: http://www.ubuntu.com/usn/usn-1601-1/
usn: 1601-1
cert-bund: CB-K16/1107
cert-bund: CB-K14/1065
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2014-1114
dfn-cert: DFN-CERT-2013-0695
dfn-cert: DFN-CERT-2012-2161
dfn-cert: DFN-CERT-2012-2081
dfn-cert: DFN-CERT-2012-2028
dfn-cert: DFN-CERT-2012-2027
dfn-cert: DFN-CERT-2012-2026
dfn-cert: DFN-CERT-2012-2014
dfn-cert: DFN-CERT-2012-2009
dfn-cert: DFN-CERT-2012-2008
dfn-cert: DFN-CERT-2012-2007
dfn-cert: DFN-CERT-2012-1969
dfn-cert: DFN-CERT-2012-1965
dfn-cert: DFN-CERT-2012-1964
dfn-cert: DFN-CERT-2012-1958
```

High (CVSS: 7.8)
NVT: Ubuntu Update for linux vulnerabilities USN-1105-1

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Ubuntu Update for Linux kernel vulnerabilities USN-1105-1

Vulnerability Detection Result

```
Vulnerable package: linux-libc-dev
Installed version:  2.6.24-27.68
Fixed version:      2.6.24-29.88
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

linux vulnerabilities on Ubuntu 8.04 LTS

Vulnerability Insight

Dan Rosenberg discovered that multiple terminal ioctls did not correctly initialize structure memory. A local attacker could exploit this to read portions of kernel stack memory, leading to a loss of privacy. (CVE-2010-4075, CVE-2010-4076, CVE-2010-4077)

Dan Rosenberg discovered that the socket filters did not correctly initialize structure memory. A local attacker could create malicious filters to read portions of kernel stack memory, leading to a loss of privacy. (CVE-2010-4158)

Dan Rosenberg discovered that certain iovec operations did not calculate page counts correctly. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-4162)

Dan Rosenberg discovered that the SCSI subsystem did not correctly validate iov segments. A local attacker with access to a SCSI device could send specially crafted requests to crash the system, leading to a denial of service. (CVE-2010-4163)

Dan Rosenberg discovered multiple flaws in the X.25 facilities parsing. If a system was using X.25, a remote attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-4164)

Alan Cox discovered that the HCI UART driver did not correctly check if a write operation was available. A local attacker could exploit this flaw to gain root privileges. (CVE-2010-4242)

Nelson Elhage discovered that the kernel did not correctly handle process cleanup after triggering a recoverable kernel bug. If a local attacker were able to trigger certain kinds of kernel bugs, they could create a specially crafted process to gain root privileges. (CVE-2010-4258)

Tavis Ormandy discovered that the install_special_mapping function could bypass the mmap_min_addr restriction. A local attacker could exploit this to mmap 4096 bytes below the mmap_min_addr area, possibly improving the chances of performing NULL pointer dereference attacks. (CVE-2010-4346)

Vulnerability Detection Method

Details: `Ubuntu Update for linux vulnerabilities USN-1105-1`

OID:1.3.6.1.4.1.25623.1.0.840632

Version used: `2019-03-13T09:25:59Z`

References

`cve: CVE-2010-4075`

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2010-4076
cve: CVE-2010-4077
cve: CVE-2010-4158
cve: CVE-2010-4162
cve: CVE-2010-4163
cve: CVE-2010-4164
cve: CVE-2010-4242
cve: CVE-2010-4258
cve: CVE-2010-4346
url: http://www.ubuntu.com/usn/usn-1105-1/
usn: 1105-1
dfn-cert: DFN-CERT-2013-1066
dfn-cert: DFN-CERT-2012-2075
dfn-cert: DFN-CERT-2012-1272
dfn-cert: DFN-CERT-2012-0209
dfn-cert: DFN-CERT-2012-0204
dfn-cert: DFN-CERT-2011-1594
dfn-cert: DFN-CERT-2011-0979
dfn-cert: DFN-CERT-2011-0964
dfn-cert: DFN-CERT-2011-0676
dfn-cert: DFN-CERT-2011-0598
dfn-cert: DFN-CERT-2011-0571
dfn-cert: DFN-CERT-2011-0525
dfn-cert: DFN-CERT-2011-0443
dfn-cert: DFN-CERT-2011-0351
dfn-cert: DFN-CERT-2011-0338
dfn-cert: DFN-CERT-2011-0324
dfn-cert: DFN-CERT-2011-0225
dfn-cert: DFN-CERT-2011-0187
dfn-cert: DFN-CERT-2011-0186
dfn-cert: DFN-CERT-2011-0150
dfn-cert: DFN-CERT-2011-0134
dfn-cert: DFN-CERT-2011-0110
dfn-cert: DFN-CERT-2011-0077
dfn-cert: DFN-CERT-2011-0065
dfn-cert: DFN-CERT-2011-0050
dfn-cert: DFN-CERT-2011-0042
dfn-cert: DFN-CERT-2011-0008
dfn-cert: DFN-CERT-2011-0005
dfn-cert: DFN-CERT-2011-0004
dfn-cert: DFN-CERT-2010-1761
dfn-cert: DFN-CERT-2010-1715
dfn-cert: DFN-CERT-2010-1668
dfn-cert: DFN-CERT-2010-1657
dfn-cert: DFN-CERT-2010-1646
dfn-cert: DFN-CERT-2010-1623
```

High (CVSS: 7.6)
NVT: Ubuntu Update for pango1.0 vulnerabilities USN-1082-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1082-1

Vulnerability Detection Result

```
Vulnerable package: libpango1.0-0
Installed version:  1.20.5-0ubuntu1.1
Fixed version:      1.20.5-0ubuntu1.2
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
pango1.0 vulnerabilities on Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight
Marc Schoenefeld discovered that Pango incorrectly handled certain Glyph Definition (GDEF) tables. If a user were tricked into displaying text with a specially-crafted font, an attacker could cause Pango to crash, resulting in a denial of service. This issue only affected Ubuntu 8.04 LTS and 9.10. (CVE-2010-0421)
Dan Rosenberg discovered that Pango incorrectly handled certain FT_Bitmap objects. If a user were tricked into displaying text with a specially- crafted font, an attacker could cause a denial of service or execute arbitrary code with privileges of the user invoking the program. The default compiler options for affected releases should reduce the vulnerability to a denial of service. (CVE-2011-0020)
It was discovered that Pango incorrectly handled certain memory reallocation failures. If a user were tricked into displaying text in a way that would cause a reallocation failure, an attacker could cause a denial of service or execute arbitrary code with privileges of the user invoking the program. This issue only affected Ubuntu 9.10, 10.04 LTS and 10.10. (CVE-2011-0064)

Vulnerability Detection Method
Details: `Ubuntu Update for pango1.0 vulnerabilities USN-1082-1`
OID:1.3.6.1.4.1.25623.1.0.840602
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2010-0421
cve: CVE-2011-0020
cve: CVE-2011-0064
url: http://www.ubuntu.com/usn/usn-1082-1/
usn: 1082-1
dfn-cert: DFN-CERT-2011-0492
dfn-cert: DFN-CERT-2011-0383
dfn-cert: DFN-CERT-2011-0297
dfn-cert: DFN-CERT-2011-0284
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-0277
dfn-cert: DFN-CERT-2011-0145
dfn-cert: DFN-CERT-2011-0123
dfn-cert: DFN-CERT-2010-0813
dfn-cert: DFN-CERT-2010-0775
dfn-cert: DFN-CERT-2010-0705
dfn-cert: DFN-CERT-2010-0542
dfn-cert: DFN-CERT-2010-0381
dfn-cert: DFN-CERT-2010-0351
```

High (CVSS: 7.5)
NVT: Ubuntu Update for php5 USN-1358-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1358-1

Vulnerability Detection Result

```
Vulnerable package: php5-cgi
Installed version:  5.2.4-2ubuntu5.10
Fixed version:      5.2.4-2ubuntu5.22
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
php5 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that PHP computed hash values for form parameters without restricting the ability to trigger hash collisions predictably. This could allow a remote attacker to cause a denial of service by sending many crafted parameters. (CVE-2011-4885)
ATTENTION: this update changes previous PHP behavior by limiting the number of external input variables to 1000. This may be increased by adding a 'max_input_vars' directive to the php.ini configuration file. See the references for more information.
Stefan Esser discovered that the fix to address the predictable hash collision issue, CVE-2011-4885, did not properly handle the situation where the limit was reached. This could allow a remote attacker to cause a denial of service or execute arbitrary code via a request containing a large number of variables. (CVE-2012-0830)
It was discovered that PHP did not always check the return value of the zend_strndup function. This could allow a remote attacker to cause a denial of service. (CVE-2011-4153)
It was discovered that PHP did not properly enforce libxslt security settings. This could allow a remote attacker to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension. (CVE-2012-0057)
It was discovered that PHP did not properly enforce that PDORow objects could not be serialized and not be saved in a session. A remote attacker could use this to cause a denial of service via an application crash. (CVE-2012-0788)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that PHP allowed the magic_quotes_gpc setting to be disabled remotely. This could allow a remote attacker to bypass restrictions that could prevent an SQL injection. (CVE-2012-0831)
USN 1126-1 addressed an issue where the /etc/cron.d/php5 cron job for PHP allowed local users to delete arbitrary files via a symlink attack on a directory under /var/lib/php5/. Emese Revfy discovered that the fix had not been applied to PHP for Ubuntu 10.04 LTS. This update corrects the issue. We apologize for the error. (CVE-2011-0441)

Vulnerability Detection Method
Details: `Ubuntu Update for php5 USN-1358-1`
OID:1.3.6.1.4.1.25623.1.0.840891
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-4885
cve: CVE-2012-0830
cve: CVE-2011-4153
cve: CVE-2012-0057
cve: CVE-2012-0788
cve: CVE-2012-0831
cve: CVE-2011-0441
url: http://www.ubuntu.com/usn/usn-1358-1/
usn: 1358-1
url: http://www.php.net/manual/en/info.configuration.php#ini.max-input-vars
cert-bund: CB-K13/0712
dfn-cert: DFN-CERT-2013-1713
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2013-0357
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1268
dfn-cert: DFN-CERT-2012-1267
dfn-cert: DFN-CERT-2012-1266
dfn-cert: DFN-CERT-2012-1173
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0870
dfn-cert: DFN-CERT-2012-0869
dfn-cert: DFN-CERT-2012-0813
dfn-cert: DFN-CERT-2012-0714
dfn-cert: DFN-CERT-2012-0641
dfn-cert: DFN-CERT-2012-0586
dfn-cert: DFN-CERT-2012-0538
dfn-cert: DFN-CERT-2012-0268
dfn-cert: DFN-CERT-2012-0267
dfn-cert: DFN-CERT-2012-0266
dfn-cert: DFN-CERT-2012-0265
dfn-cert: DFN-CERT-2012-0214
dfn-cert: DFN-CERT-2012-0213
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0211
dfn-cert: DFN-CERT-2012-0210
dfn-cert: DFN-CERT-2012-0197
dfn-cert: DFN-CERT-2012-0196
dfn-cert: DFN-CERT-2012-0195
dfn-cert: DFN-CERT-2012-0172
dfn-cert: DFN-CERT-2012-0167
dfn-cert: DFN-CERT-2012-0165
dfn-cert: DFN-CERT-2012-0149
dfn-cert: DFN-CERT-2012-0130
dfn-cert: DFN-CERT-2012-0111
dfn-cert: DFN-CERT-2012-0099
dfn-cert: DFN-CERT-2012-0070
dfn-cert: DFN-CERT-2012-0003
dfn-cert: DFN-CERT-2011-0530
dfn-cert: DFN-CERT-2011-0402
```

High (CVSS: 7.5)
NVT: Ubuntu Update for eglibc USN-1396-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1396-1

Vulnerability Detection Result

```
Vulnerable package: libc6
Installed version:  2.7-10ubuntu5
Fixed version:      2.7-10ubuntu8.1
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
eglibc on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that the GNU C Library did not properly handle integer overflows in the timezone handling code. An attacker could use this to possibly execute arbitrary code by convincing an application to load a maliciously constructed tzfile. (CVE-2009-5029)
It was discovered that the GNU C Library did not properly handle passwd.adjunct.byname map entries in the Network Information Service (NIS) code in the name service caching daemon (nscd). An attacker could use this to obtain the encrypted passwords of NIS accounts. This issue only affected Ubuntu 8.04 LTS. (CVE-2010-0015)
Chris Evans reported that the GNU C Library did not properly calculate the amount of memory to allocate in the fnmatch() code. An attacker could use this to cause a denial of service or possibly execute arbitrary code via a maliciously crafted UTF-8 string. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS and Ubuntu 10.10. (CVE-2011-1071)

. . . continues on next page . . .

. . . continued from previous page . . .

Tomas Hoger reported that an additional integer overflow was possible in the GNU C Library fnmatch() code. An attacker could use this to cause a denial of service via a maliciously crafted UTF-8 string. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-1659)

Dan Rosenberg discovered that the addmntent() function in the GNU C Library did not report an error status for failed attempts to write to the /etc/mtab file. This could allow an attacker to corrupt /etc/mtab, possibly causing a denial of service or otherwise manipulate mount options. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-1089)

Harald van Dijk discovered that the locale program included with the GNU C library did not properly quote its output. This could allow a local attacker to possibly execute arbitrary code using a crafted localization string that was evaluated in a shell script. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS and Ubuntu 10.10. (CVE-2011-1095)

It was discovered that the GNU C library loader expanded the $ORIGIN dynamic string token when RPATH is composed entirely of this token. This could allow an attacker to gain privilege via a setuid program that had this RPATH value. (CVE-2011-1658)

It was discovered that the GNU C library implementation of memcpy optimized for Supplemental Streaming SIMD Extensions 3 (SSSE3) contained a possible integer overflow. An attacker could use this to cause a denial of service or possibly exec ...

Description truncated, please see the referenced URL(s) for more information.

Vulnerability Detection Method

Details: `Ubuntu Update for eglibc USN-1396-1`

OID:1.3.6.1.4.1.25623.1.0.840929

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2009-5029
cve: CVE-2010-0015
cve: CVE-2011-1071
cve: CVE-2011-1659
cve: CVE-2011-1089
cve: CVE-2011-1095
cve: CVE-2011-1658
cve: CVE-2011-2702
cve: CVE-2011-4609
cve: CVE-2012-0864
url: http://www.ubuntu.com/usn/usn-1396-1/
usn: 1396-1
cert-bund: CB-K16/1278
cert-bund: CB-K14/1476
dfn-cert: DFN-CERT-2016-1358
dfn-cert: DFN-CERT-2014-1559
dfn-cert: DFN-CERT-2012-2288
dfn-cert: DFN-CERT-2012-1697
dfn-cert: DFN-CERT-2012-0509
dfn-cert: DFN-CERT-2012-0490
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0440
dfn-cert: DFN-CERT-2012-0377
dfn-cert: DFN-CERT-2012-0366
dfn-cert: DFN-CERT-2012-0261
dfn-cert: DFN-CERT-2012-0260
dfn-cert: DFN-CERT-2012-0144
dfn-cert: DFN-CERT-2012-0091
dfn-cert: DFN-CERT-2012-0046
dfn-cert: DFN-CERT-2012-0031
dfn-cert: DFN-CERT-2012-0027
dfn-cert: DFN-CERT-2011-1852
dfn-cert: DFN-CERT-2011-1814
dfn-cert: DFN-CERT-2011-1813
dfn-cert: DFN-CERT-2011-1594
dfn-cert: DFN-CERT-2011-1148
dfn-cert: DFN-CERT-2011-0507
dfn-cert: DFN-CERT-2011-0505
dfn-cert: DFN-CERT-2010-1442
dfn-cert: DFN-CERT-2010-0755
dfn-cert: DFN-CERT-2010-0086
```

High (CVSS: 7.5)
NVT: Ubuntu Update for perl USN-1770-1

Summary
The remote host is missing an update for the 'perl' package(s) announced via the referenced advisory.

Vulnerability Detection Result

```
Vulnerable package: perl
Installed version:  5.8.8-12ubuntu0.5
Fixed version:      5.8.8-12ubuntu0.8
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
perl on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Yves Orton discovered that Perl incorrectly handled hashing when using user-provided hash keys. An attacker could use this flaw to perform a denial of service attack against software written in Perl.

Vulnerability Detection Method
Details: `Ubuntu Update for perl USN-1770-1`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.841369
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2013-1667
url: http://www.ubuntu.com/usn/usn-1770-1/
usn: 1770-1
cert-bund: CB-K16/1107
cert-bund: CB-K16/0564
cert-bund: CB-K15/1514
cert-bund: CB-K13/0845
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-0872
dfn-cert: DFN-CERT-2013-0668
dfn-cert: DFN-CERT-2013-0648
dfn-cert: DFN-CERT-2013-0628
dfn-cert: DFN-CERT-2013-0617
dfn-cert: DFN-CERT-2013-0611
dfn-cert: DFN-CERT-2013-0560
dfn-cert: DFN-CERT-2013-0559
dfn-cert: DFN-CERT-2013-0517
```

High (CVSS: 7.5)
NVT: Ubuntu Update for perl USN-1643-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1643-1

Vulnerability Detection Result

```
Vulnerable package: perl
Installed version:  5.8.8-12ubuntu0.5
Fixed version:      5.8.8-12ubuntu0.7
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
perl on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that the decode_xs function in the Encode module is vulnerable to a heap-based buffer overflow via a crafted Unicode string. An attacker could use this overflow to cause a denial of service. (CVE-2011-2939)
It was discovered that the 'new' constructor in the Digest module is vulnerable to an eval injection. An attacker could use this to execute arbitrary code. (CVE-2011-3597)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that Perl's 'x' string repeat operator is vulnerable to a heap-based buffer overflow. An attacker could use this to execute arbitrary code. (CVE-2012-5195)
Ryo Anazawa discovered that the CGI.pm module does not properly escape newlines in Set-Cookie or P3P (Platform for Privacy Preferences Project) headers. An attacker could use this to inject arbitrary headers into responses from applications that use CGI.pm. (CVE-2012-5526)

Vulnerability Detection Method
Details: `Ubuntu Update for perl USN-1643-1`
OID:1.3.6.1.4.1.25623.1.0.841232
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-2939
cve: CVE-2011-3597
cve: CVE-2012-5195
cve: CVE-2012-5526
url: http://www.ubuntu.com/usn/usn-1643-1/
usn: 1643-1
cert-bund: CB-K16/1107
cert-bund: CB-K16/0564
cert-bund: CB-K15/1514
cert-bund: CB-K14/1466
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2014-1550
dfn-cert: DFN-CERT-2013-1230
dfn-cert: DFN-CERT-2013-0989
dfn-cert: DFN-CERT-2013-0944
dfn-cert: DFN-CERT-2013-0648
dfn-cert: DFN-CERT-2013-0617
dfn-cert: DFN-CERT-2013-0611
dfn-cert: DFN-CERT-2013-0560
dfn-cert: DFN-CERT-2013-0559
dfn-cert: DFN-CERT-2012-2271
dfn-cert: DFN-CERT-2012-2244
dfn-cert: DFN-CERT-2012-2239
dfn-cert: DFN-CERT-2012-2238
dfn-cert: DFN-CERT-2012-2178
dfn-cert: DFN-CERT-2012-1697
dfn-cert: DFN-CERT-2012-1345
dfn-cert: DFN-CERT-2012-0094
dfn-cert: DFN-CERT-2012-0093
dfn-cert: DFN-CERT-2012-0016
dfn-cert: DFN-CERT-2011-1870
dfn-cert: DFN-CERT-2011-1691
dfn-cert: DFN-CERT-2011-1681
```

High (CVSS: 7.5)
NVT: Ubuntu Update for php5 USN-1126-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1126-1

Vulnerability Detection Result

```
Vulnerable package: php5-cgi
Installed version:  5.2.4-2ubuntu5.10
Fixed version:      5.2.4-2ubuntu5.15
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
php5 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 9.10, Ubuntu 8.04 LTS, Ubuntu 6.06 LTS

Vulnerability Insight
Stephane Chazelas discovered that the /etc/cron.d/php5 cron job for PHP 5.3.5 allows local users to delete arbitrary files via a symlink attack on a directory under /var/lib/php5/. (CVE-2011-0441)
Raphael Geisert and Dan Rosenberg discovered that the PEAR installer allows local users to overwrite arbitrary files via a symlink attack on the package.xml file, related to the (1) download_dir, (2) cache_dir, (3) tmp_dir, and (4) pear-build-download directories. (CVE-2011-1072, CVE-2011-1144)
Ben Schmidt discovered that a use-after-free vulnerability in the PHP Zend engine could allow an attacker to cause a denial of service (heap memory corruption) or possibly execute arbitrary code. (CVE-2010-4697)
Martin Barbella discovered a buffer overflow in the PHP GD extension that allows an attacker to cause a denial of service (application crash) via a large number of anti- aliasing steps in an argument to the imagepstext function. (CVE-2010-4698)
It was discovered that PHP accepts the \0 character in a pathname, which might allow an attacker to bypass intended access restrictions by placing a safe file extension after this character. This issue is addressed in Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2006-7243)
Maksymilian Arciemowicz discovered that the grapheme_extract function in the PHP Internationalization extension (Intl) for ICU allow an attacker to cause a denial of service (crash) via an invalid size argument, which triggers a NULL pointer dereference. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-0420)
Maksymilian Arciemowicz discovered that the _zip_name_locate function in the PHP Zip extension does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow an attacker to cause a denial of service (NULL pointer dereference) via an empty ZIP archive. This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-0421)
Luca Carettoni discovered that the PHP Exif extension performs an incorrect cast on 64bit platforms, which allows a remote attacker to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD). (CVE-2011-0708)

. . . continues on next page . . .

. . . continued from previous page . . .

Jose Carlos Norte discovered that an integer overflow in the PHP shmop extension could allow an attacker to cause a denial of service (crash) and possibly read sensitive memory function. (CVE-2011-1092)

Felipe Pena discovered that ...

Description truncated, please see the referenced URL(s) for more information.

Vulnerability Detection Method

Details: `Ubuntu Update for php5 USN-1126-1`

OID:1.3.6.1.4.1.25623.1.0.840646

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-0441
cve: CVE-2011-1072
cve: CVE-2011-1144
cve: CVE-2010-4697
cve: CVE-2010-4698
cve: CVE-2006-7243
cve: CVE-2011-0420
cve: CVE-2011-0421
cve: CVE-2011-0708
cve: CVE-2011-1092
cve: CVE-2011-1148
cve: CVE-2011-1153
cve: CVE-2011-1464
cve: CVE-2011-1466
cve: CVE-2011-1467
cve: CVE-2011-1468
cve: CVE-2011-1469
cve: CVE-2011-1470
cve: CVE-2011-1471
url: http://www.ubuntu.com/usn/usn-1126-1/
usn: 1126-1
cert-bund: CB-K16/0944
cert-bund: CB-K15/0703
cert-bund: CB-K14/0323
cert-bund: CB-K13/0712
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2015-0732
dfn-cert: DFN-CERT-2014-0336
dfn-cert: DFN-CERT-2013-1713
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0731
dfn-cert: DFN-CERT-2012-0714
dfn-cert: DFN-CERT-2012-0586
dfn-cert: DFN-CERT-2012-0268
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0210
dfn-cert: DFN-CERT-2012-0165
dfn-cert: DFN-CERT-2012-0099
dfn-cert: DFN-CERT-2011-1924
dfn-cert: DFN-CERT-2011-1851
dfn-cert: DFN-CERT-2011-1698
dfn-cert: DFN-CERT-2011-1686
dfn-cert: DFN-CERT-2011-1443
dfn-cert: DFN-CERT-2011-1433
dfn-cert: DFN-CERT-2011-1402
dfn-cert: DFN-CERT-2011-1396
dfn-cert: DFN-CERT-2011-1387
dfn-cert: DFN-CERT-2011-1005
dfn-cert: DFN-CERT-2011-0807
dfn-cert: DFN-CERT-2011-0771
dfn-cert: DFN-CERT-2011-0530
dfn-cert: DFN-CERT-2011-0520
dfn-cert: DFN-CERT-2011-0518
dfn-cert: DFN-CERT-2011-0517
dfn-cert: DFN-CERT-2011-0515
dfn-cert: DFN-CERT-2011-0445
dfn-cert: DFN-CERT-2011-0444
dfn-cert: DFN-CERT-2011-0442
dfn-cert: DFN-CERT-2011-0441
dfn-cert: DFN-CERT-2011-0432
dfn-cert: DFN-CERT-2011-0402
dfn-cert: DFN-CERT-2011-0013
dfn-cert: DFN-CERT-2011-0012
dfn-cert: DFN-CERT-2011-0011
dfn-cert: DFN-CERT-2010-1729
```

High (CVSS: 7.5)
NVT: Ubuntu Update for php5 USN-1231-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1231-1

Vulnerability Detection Result

```
Vulnerable package: php5-cgi
Installed version:  5.2.4-2ubuntu5.10
Fixed version:      5.2.4-2ubuntu5.18
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

php5 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

Mateusz Kocielski, Marek Kroemeke and Filip Palian discovered that a stack-based buffer overflow existed in the socket_connect function's handling of long pathnames for AF_UNIX sockets. A remote attacker might be able to exploit this to execute arbitrary code. However, the default compiler options for affected releases should reduce the vulnerability to a denial of service. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-1938)

Krzysztof Kotowicz discovered that the PHP post handler function does not properly restrict filenames in multipart/form-data POST requests. This may allow remote attackers to conduct absolute path traversal attacks and possibly create or overwrite arbitrary files. This issue affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-2202)

It was discovered that the crypt function for blowfish does not properly handle 8-bit characters. This could make it easier for an attacker to discover a cleartext password containing an 8-bit character that has a matching blowfish crypt value. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-2483)

It was discovered that PHP did not properly check the return values of the malloc(3), calloc(3) and realloc(3) library functions in multiple locations. This could allow an attacker to cause a denial of service via a NULL pointer dereference or possibly execute arbitrary code. This issue affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-3182)

Maksymilian Arciemowicz discovered that PHP did not properly implement the error_log function. This could allow an attacker to cause a denial of service via an application crash. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, Ubuntu 11.04 and Ubuntu 11.10. (CVE-2011-3267)

Maksymilian Arciemowicz discovered that the ZipArchive functions addGlob() and addPattern() did not properly check their flag arguments. This could allow a malicious script author to cause a denial of service via application crash. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, Ubuntu 11.04 and Ubuntu 11.10. (CVE-2011-1657)

It was discovered that the Xend opcode parser in PHP could be interrupted while handling the shift-left, shift-right, and bitwise-xor opcodes. This could allow a malicious script author to expose memory contents. This issue affected Ubuntu 10.04 LTS. (CVE-2010-1914)

It was discovered that the strrchr function in PHP could be interrupted by a malicious script, allowing the exposure of memory contents. This issue affected Ubuntu 8.04 LTS. (CVE-2010-2484)

Vulnerability Detection Method

Details: `Ubuntu Update for php5 USN-1231-1`

OID:1.3.6.1.4.1.25623.1.0.840782

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-1938
cve: CVE-2011-2202
cve: CVE-2011-2483
cve: CVE-2011-3182
cve: CVE-2011-3267
cve: CVE-2011-1657
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2010-1914
cve: CVE-2010-2484
url: http://www.ubuntu.com/usn/usn-1231-1/
usn: 1231-1
cert-bund: CB-K15/1514
cert-bund: CB-K13/0921
dfn-cert: DFN-CERT-2013-1938
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0731
dfn-cert: DFN-CERT-2012-0714
dfn-cert: DFN-CERT-2012-0678
dfn-cert: DFN-CERT-2012-0172
dfn-cert: DFN-CERT-2012-0167
dfn-cert: DFN-CERT-2012-0165
dfn-cert: DFN-CERT-2012-0099
dfn-cert: DFN-CERT-2011-1816
dfn-cert: DFN-CERT-2011-1814
dfn-cert: DFN-CERT-2011-1813
dfn-cert: DFN-CERT-2011-1708
dfn-cert: DFN-CERT-2011-1698
dfn-cert: DFN-CERT-2011-1686
dfn-cert: DFN-CERT-2011-1643
dfn-cert: DFN-CERT-2011-1603
dfn-cert: DFN-CERT-2011-1602
dfn-cert: DFN-CERT-2011-1443
dfn-cert: DFN-CERT-2011-1433
dfn-cert: DFN-CERT-2011-1402
dfn-cert: DFN-CERT-2011-1396
dfn-cert: DFN-CERT-2011-1387
dfn-cert: DFN-CERT-2011-1276
dfn-cert: DFN-CERT-2011-1005
dfn-cert: DFN-CERT-2011-0642
dfn-cert: DFN-CERT-2010-1620
dfn-cert: DFN-CERT-2010-1321
dfn-cert: DFN-CERT-2010-1247
dfn-cert: DFN-CERT-2010-1079
dfn-cert: DFN-CERT-2010-0997
dfn-cert: DFN-CERT-2010-0953
```

High (CVSS: 7.5)
NVT: Ubuntu Update for php5 USN-1126-2

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1126-2

Vulnerability Detection Result

... continues on next page ...

. . . continued from previous page . . .

```
Vulnerable package: php5-cgi
Installed version:  5.2.4-2ubuntu5.10
Fixed version:      5.2.4-2ubuntu5.17
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
php5 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 9.10, Ubuntu 8.04 LTS, Ubuntu 6.06 LTS

Vulnerability Insight
USN 1126-1 fixed several vulnerabilities in PHP. The fix for CVE-2010-4697 introduced an incorrect reference counting regression in the Zend engine that caused the PHP interpreter to segfault. This regression affects Ubuntu 6.06 LTS and Ubuntu 8.04 LTS.
The fixes for CVE-2011-1072 and CVE-2011-1144 introduced a regression in the PEAR installer that prevented it from creating its cache directory and reporting errors correctly.
We apologize for the inconvenience.
Original advisory details:
Stephane Chazelas discovered that the /etc/cron.d/php5 cron job for PHP 5.3.5 allows local users to delete arbitrary files via a symlink attack on a directory under /var/lib/php5/. (CVE-2011-0441)
Raphael Geisert and Dan Rosenberg discovered that the PEAR installer allows local users to overwrite arbitrary files via a symlink attack on the package.xml file, related to the (1) download_dir, (2) cache_dir, (3) tmp_dir, and (4) pear-build-download directories. (CVE-2011-1072, CVE-2011-1144)
Ben Schmidt discovered that a use-after-free vulnerability in the PHP Zend engine could allow an attacker to cause a denial of service (heap memory corruption) or possibly execute arbitrary code. (CVE-2010-4697)
Martin Barbella discovered a buffer overflow in the PHP GD extension that allows an attacker to cause a denial of service (application crash) via a large number of anti- aliasing steps in an argument to the imagepstext function. (CVE-2010-4698)
It was discovered that PHP accepts the \0 character in a pathname, which might allow an attacker to bypass intended access restrictions by placing a safe file extension after this character. This issue is addressed in Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2006-7243)
Maksymilian Arciemowicz discovered that the grapheme_extract function in the PHP Internationalization extension (Intl) for ICU allow an attacker to cause a denial of service (crash) via an invalid size argument, which triggers a NULL pointer dereference. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-0420)
Maksymilian Arciemowicz discovered that the _zip_name_locate function in the PHP Zip extension does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow an attacker to cause a denial of service (NULL pointer dereference) via an empty ZIP archive. This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (...
Description truncated, please see the referenced URL(s) for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Details: Ubuntu Update for php5 USN-1126-2

OID:1.3.6.1.4.1.25623.1.0.840636

Version used: 2019-03-13T09:25:59Z

References

```
cve: CVE-2010-4697
cve: CVE-2011-1072
cve: CVE-2011-1144
cve: CVE-2011-0441
cve: CVE-2010-4698
cve: CVE-2006-7243
cve: CVE-2011-0420
cve: CVE-2011-0421
cve: CVE-2011-0708
cve: CVE-2011-1092
cve: CVE-2011-1148
cve: CVE-2011-1153
cve: CVE-2011-1464
cve: CVE-2011-1466
cve: CVE-2011-1467
cve: CVE-2011-1468
cve: CVE-2011-1469
cve: CVE-2011-1470
cve: CVE-2011-1471
url: http://www.ubuntu.com/usn/usn-1126-2/
usn: 1126-2
cert-bund: CB-K16/0944
cert-bund: CB-K15/0703
cert-bund: CB-K14/0323
cert-bund: CB-K13/0712
dfn-cert: DFN-CERT-2016-1004
dfn-cert: DFN-CERT-2015-0732
dfn-cert: DFN-CERT-2014-0336
dfn-cert: DFN-CERT-2013-1713
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0731
dfn-cert: DFN-CERT-2012-0714
dfn-cert: DFN-CERT-2012-0586
dfn-cert: DFN-CERT-2012-0268
dfn-cert: DFN-CERT-2012-0210
dfn-cert: DFN-CERT-2012-0165
dfn-cert: DFN-CERT-2012-0099
dfn-cert: DFN-CERT-2011-1924
dfn-cert: DFN-CERT-2011-1851
dfn-cert: DFN-CERT-2011-1698
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-1686
dfn-cert: DFN-CERT-2011-1443
dfn-cert: DFN-CERT-2011-1433
dfn-cert: DFN-CERT-2011-1402
dfn-cert: DFN-CERT-2011-1396
dfn-cert: DFN-CERT-2011-1387
dfn-cert: DFN-CERT-2011-1005
dfn-cert: DFN-CERT-2011-0807
dfn-cert: DFN-CERT-2011-0771
dfn-cert: DFN-CERT-2011-0530
dfn-cert: DFN-CERT-2011-0520
dfn-cert: DFN-CERT-2011-0518
dfn-cert: DFN-CERT-2011-0517
dfn-cert: DFN-CERT-2011-0515
dfn-cert: DFN-CERT-2011-0445
dfn-cert: DFN-CERT-2011-0444
dfn-cert: DFN-CERT-2011-0442
dfn-cert: DFN-CERT-2011-0441
dfn-cert: DFN-CERT-2011-0432
dfn-cert: DFN-CERT-2011-0402
dfn-cert: DFN-CERT-2011-0013
dfn-cert: DFN-CERT-2011-0012
dfn-cert: DFN-CERT-2011-0011
dfn-cert: DFN-CERT-2010-1729
```

High (CVSS: 7.5)
NVT: Ubuntu Update for php5 USN-1437-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1437-1

Vulnerability Detection Result

```
Vulnerable package: php5-cgi
Installed version:  5.2.4-2ubuntu5.10
Fixed version:      5.2.4-2ubuntu5.24
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
php5 on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that PHP, when used as a stand alone CGI processor for the Apache Web Server, did not properly parse and filter query strings. This could allow a remote attacker to execute arbitrary code running with the privilege of the web server. Configurations using mod_php5 and FastCGI were not vulnerable.

This update addresses the issue when the PHP CGI interpreter is configured using mod_cgi and mod_actions as described in /usr/share/doc/php5-cgi/README.Debian.gz. However, if an alternate configuration is used to enable PHP CGI processing, it should be reviewed to ensure that command line arguments cannot be passed to the PHP interpreter. Please see the references for more details and potential mitigation approaches.

Vulnerability Detection Method

Details: `Ubuntu Update for php5 USN-1437-1`

OID:1.3.6.1.4.1.25623.1.0.841002

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-2311
cve: CVE-2012-1823
url: http://www.ubuntu.com/usn/usn-1437-1/
usn: 1437-1
url: http://people.canonical.com/~ubuntu-security/cve/2012/CVE-2012-2311.html
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1268
dfn-cert: DFN-CERT-2012-1267
dfn-cert: DFN-CERT-2012-1266
dfn-cert: DFN-CERT-2012-1173
dfn-cert: DFN-CERT-2012-0994
dfn-cert: DFN-CERT-2012-0993
dfn-cert: DFN-CERT-2012-0992
dfn-cert: DFN-CERT-2012-0920
dfn-cert: DFN-CERT-2012-0915
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0913
dfn-cert: DFN-CERT-2012-0907
dfn-cert: DFN-CERT-2012-0906
dfn-cert: DFN-CERT-2012-0900
dfn-cert: DFN-CERT-2012-0880
dfn-cert: DFN-CERT-2012-0878
```

High (CVSS: 7.5)
NVT: Ubuntu Update for php5 USN-1358-2

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1358-2

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable package: php5-cgi
Installed version:  5.2.4-2ubuntu5.10
Fixed version:      5.2.4-2ubuntu5.23
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
php5 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
USN 1358-1 fixed multiple vulnerabilities in PHP. The fix for CVE-2012-0831 introduced a regression where the state of the magic_quotes_gpc setting was not correctly reflected when calling the ini_get() function.
We apologize for the inconvenience.
Original advisory details:
It was discovered that PHP computed hash values for form parameters without restricting the ability to trigger hash collisions predictably. This could allow a remote attacker to cause a denial of service by sending many crafted parameters. (CVE-2011-4885)
ATTENTION: this update changes previous PHP behavior by limiting the number of external input variables to 1000. This may be increased by adding a 'max_input_vars' directive to the php.ini configuration file. See the references for more information.
Stefan Esser discovered that the fix to address the predictable hash collision issue, CVE-2011-4885, did not properly handle the situation where the limit was reached. This could allow a remote attacker to cause a denial of service or execute arbitrary code via a request containing a large number of variables. (CVE-2012-0830)
It was discovered that PHP did not always check the return value of the zend_strndup function. This could allow a remote attacker to cause a denial of service. (CVE-2011-4153)
It was discovered that PHP did not properly enforce libxslt security settings. This could allow a remote attacker to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension. (CVE-2012-0057)
It was discovered that PHP did not properly enforce that PDORow objects could not be serialized and not be saved in a session. A remote attacker could use this to cause a denial of service via an application crash. (CVE-2012-0788)
It was discovered that PHP allowed the magic_quotes_gpc setting to be disabled remotely. This could allow a remote attacker to bypass restrictions that could prevent an SQL injection. (CVE-2012-0831)
USN 1126-1 addressed an issue where the /etc/cron.d/php5 cron job for PHP allowed local users to delete arbitrary files via a symlink attack on a directory under /var/lib/php5/. Emese Revfy discovered that the fix had not been applied to PHP for Ubuntu 10.04 LTS. This update corrects the issue. We apologize for the error. (CVE-2011-0441)

Vulnerability Detection Method
Details: `Ubuntu Update for php5 USN-1358-2`
OID:1.3.6.1.4.1.25623.1.0.840895
Version used: `2019-03-13T09:25:59Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2012-0831
cve: CVE-2011-4885
cve: CVE-2012-0830
cve: CVE-2011-4153
cve: CVE-2012-0057
cve: CVE-2012-0788
cve: CVE-2011-0441
url: http://www.ubuntu.com/usn/usn-1358-2/
usn: 1358-2
url: http://www.php.net/manual/en/info.configuration.php#ini.max-input-vars
cert-bund: CB-K13/0712
dfn-cert: DFN-CERT-2013-1713
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2013-0357
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1268
dfn-cert: DFN-CERT-2012-1267
dfn-cert: DFN-CERT-2012-1266
dfn-cert: DFN-CERT-2012-1173
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0870
dfn-cert: DFN-CERT-2012-0869
dfn-cert: DFN-CERT-2012-0813
dfn-cert: DFN-CERT-2012-0714
dfn-cert: DFN-CERT-2012-0641
dfn-cert: DFN-CERT-2012-0586
dfn-cert: DFN-CERT-2012-0538
dfn-cert: DFN-CERT-2012-0268
dfn-cert: DFN-CERT-2012-0267
dfn-cert: DFN-CERT-2012-0266
dfn-cert: DFN-CERT-2012-0265
dfn-cert: DFN-CERT-2012-0214
dfn-cert: DFN-CERT-2012-0213
dfn-cert: DFN-CERT-2012-0211
dfn-cert: DFN-CERT-2012-0210
dfn-cert: DFN-CERT-2012-0197
dfn-cert: DFN-CERT-2012-0196
dfn-cert: DFN-CERT-2012-0195
dfn-cert: DFN-CERT-2012-0172
dfn-cert: DFN-CERT-2012-0167
dfn-cert: DFN-CERT-2012-0165
dfn-cert: DFN-CERT-2012-0149
dfn-cert: DFN-CERT-2012-0130
dfn-cert: DFN-CERT-2012-0111
dfn-cert: DFN-CERT-2012-0099
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0070
dfn-cert: DFN-CERT-2012-0003
dfn-cert: DFN-CERT-2011-0530
dfn-cert: DFN-CERT-2011-0402
```

High (CVSS: 7.5)
NVT: Ubuntu Update for dhcp3 vulnerability USN-1108-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1108-1

Vulnerability Detection Result

```
Vulnerable package: dhcp3-client
Installed version:  3.0.6.dfsg-1ubuntu9
Fixed version:      3.0.6.dfsg-1ubuntu9.2
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
dhcp3 vulnerability on Ubuntu 6.06 LTS, Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight
Sebastian Krahmer discovered that the dhclient utility incorrectly filtered crafted responses. An attacker could use this flaw with a malicious DHCP server to execute arbitrary code, resulting in root privilege escalation.

Vulnerability Detection Method
Details: `Ubuntu Update for dhcp3 vulnerability USN-1108-1`
OID:1.3.6.1.4.1.25623.1.0.840633
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-0997
url: http://www.ubuntu.com/usn/usn-1108-1/
usn: 1108-1
dfn-cert: DFN-CERT-2012-0514
dfn-cert: DFN-CERT-2011-1356
dfn-cert: DFN-CERT-2011-1148
dfn-cert: DFN-CERT-2011-0850
dfn-cert: DFN-CERT-2011-0712
dfn-cert: DFN-CERT-2011-0668
dfn-cert: DFN-CERT-2011-0608
dfn-cert: DFN-CERT-2011-0599
dfn-cert: DFN-CERT-2011-0587
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-0575
dfn-cert: DFN-CERT-2011-0540
dfn-cert: DFN-CERT-2011-0539
dfn-cert: DFN-CERT-2011-0538
dfn-cert: DFN-CERT-2011-0513
```

High (CVSS: 7.5)
NVT: Ubuntu Update for tiff USN-1498-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1498-1

Vulnerability Detection Result

```
Vulnerable package: libtiff4
Installed version:  3.8.2-7ubuntu3.4
Fixed version:      3.8.2-7ubuntu3.12
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
tiff on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that the TIFF library incorrectly handled certain malformed TIFF images. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. (CVE-2012-2088)
It was discovered that the tiff2pdf utility incorrectly handled certain malformed TIFF images. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. (CVE-2012-2113)

Vulnerability Detection Method
Details: `Ubuntu Update for tiff USN-1498-1`
OID:1.3.6.1.4.1.25623.1.0.841073
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-2088
cve: CVE-2012-2113
url: http://www.ubuntu.com/usn/usn-1498-1/
usn: 1498-1
cert-bund: CB-K14/0283
cert-bund: CB-K13/0930
dfn-cert: DFN-CERT-2020-1473
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2014-0292
dfn-cert: DFN-CERT-2013-1950
dfn-cert: DFN-CERT-2012-1879
dfn-cert: DFN-CERT-2012-1635
dfn-cert: DFN-CERT-2012-1412
dfn-cert: DFN-CERT-2012-1365
dfn-cert: DFN-CERT-2012-1314
dfn-cert: DFN-CERT-2012-1304
dfn-cert: DFN-CERT-2012-1296
```

High (CVSS: 7.5)
NVT: Ubuntu Update for curl USN-1158-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1158-1

Vulnerability Detection Result

```
Vulnerable package: libcurl3-gnutls
Installed version:  7.18.0-1ubuntu2
Fixed version:      7.18.0-1ubuntu2.3
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
curl on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Richard Silverman discovered that when doing GSSAPI authentication, libcurl unconditionally performs credential delegation, handing the server a copy of the client's security credential. (CVE-2011-2192)
Wesley Miaw discovered that when zlib is enabled, libcurl does not properly restrict the amount of callback data sent to an application that requests automatic decompression. This might allow an attacker to cause a denial of service via an application crash or possibly execute arbitrary code with the privilege of the application. This issue only affected Ubuntu 8.04 LTS and Ubuntu 10.04 LTS. (CVE-2010-0734)
USN 818-1 fixed an issue with curl's handling of SSL certificates with zero bytes in the Common Name. Due to a packaging error, the fix for this issue was not being applied during the build. This issue only affected Ubuntu 8.04 LTS. We apologize for the error. (CVE-2009-2417)
Original advisory details:
Scott Cantor discovered that curl did not correctly handle SSL certificates with zero bytes in the Common Name. A remote attacker could exploit this to perform a man in the middle attack to view sensitive information or alter encrypted communications.

Vulnerability Detection Method
Details: `Ubuntu Update for curl USN-1158-1`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.840685
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-2192
cve: CVE-2010-0734
cve: CVE-2009-2417
url: http://www.ubuntu.com/usn/usn-1158-1/
usn: 1158-1
dfn-cert: DFN-CERT-2012-0731
dfn-cert: DFN-CERT-2012-0235
dfn-cert: DFN-CERT-2012-0171
dfn-cert: DFN-CERT-2011-1106
dfn-cert: DFN-CERT-2011-1024
dfn-cert: DFN-CERT-2011-1023
dfn-cert: DFN-CERT-2011-1014
dfn-cert: DFN-CERT-2011-0986
dfn-cert: DFN-CERT-2011-0185
dfn-cert: DFN-CERT-2010-1293
dfn-cert: DFN-CERT-2010-0437
dfn-cert: DFN-CERT-2010-0420
dfn-cert: DFN-CERT-2010-0379
dfn-cert: DFN-CERT-2009-1644
dfn-cert: DFN-CERT-2009-1231
dfn-cert: DFN-CERT-2009-1163
dfn-cert: DFN-CERT-2009-1138
dfn-cert: DFN-CERT-2009-1131
```

High (CVSS: 7.2)
NVT: Ubuntu Update for eglibc, glibc vulnerability USN-1009-2

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1009-2

Vulnerability Detection Result

```
Vulnerable package: libc6-dev
Installed version:  2.7-10ubuntu5
Fixed version:      2.7-10ubuntu8
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

eglibc, glibc vulnerability on Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

USN-1009-1 fixed vulnerabilities in the GNU C library. Colin Watson discovered that the fixes were incomplete and introduced flaws with setuid programs loading libraries that used dynamic string tokens in their RPATH. If the 'man' program was installed setuid, a local attacker could exploit this to gain 'man' user privileges, potentially leading to further privilege escalations. Default Ubuntu installations were not affected.
Original advisory details:
Tavis Ormandy discovered multiple flaws in the GNU C Library's handling of the LD_AUDIT environment variable when running a privileged binary. A local attacker could exploit this to gain root privileges. (CVE-2010-3847, CVE-2010-3856)

Vulnerability Detection Method
Details: `Ubuntu Update for eglibc, glibc vulnerability USN-1009-2`
OID:1.3.6.1.4.1.25623.1.0.840567
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2010-3847
cve: CVE-2010-3856
url: http://www.ubuntu.com/usn/usn-1009-2/
usn: 1009-2
dfn-cert: DFN-CERT-2011-0507
dfn-cert: DFN-CERT-2011-0505
dfn-cert: DFN-CERT-2011-0010
dfn-cert: DFN-CERT-2010-1545
dfn-cert: DFN-CERT-2010-1464
dfn-cert: DFN-CERT-2010-1448
dfn-cert: DFN-CERT-2010-1442
dfn-cert: DFN-CERT-2010-1426
dfn-cert: DFN-CERT-2010-1421
dfn-cert: DFN-CERT-2010-1420
dfn-cert: DFN-CERT-2010-1415
dfn-cert: DFN-CERT-2010-1413
dfn-cert: DFN-CERT-2010-1402
dfn-cert: DFN-CERT-2010-1401
dfn-cert: DFN-CERT-2010-1396
dfn-cert: DFN-CERT-2010-1392
```

High (CVSS: 7.2)
NVT: Ubuntu Update for sudo USN-1442-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1442-1

Vulnerability Detection Result

```
Vulnerable package: sudo
Installed version:  1.6.9p10-1ubuntu3
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      1.6.9p10-1ubuntu3.9
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
sudo on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that sudo incorrectly handled network masks when using Host and Host_List. A local user who is listed in sudoers may be allowed to run commands on unintended hosts when IPv4 network masks are used to grant access. A local attacker could exploit this to bypass intended access restrictions. Host and Host_List are not used in the default installation of Ubuntu.

Vulnerability Detection Method
Details: `Ubuntu Update for sudo USN-1442-1`
OID:1.3.6.1.4.1.25623.1.0.841006
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-2337
url: http://www.ubuntu.com/usn/usn-1442-1/
usn: 1442-1
cert-bund: CB-K13/0993
dfn-cert: DFN-CERT-2013-2029
dfn-cert: DFN-CERT-2013-1044
dfn-cert: DFN-CERT-2012-1398
dfn-cert: DFN-CERT-2012-1371
dfn-cert: DFN-CERT-2012-1356
dfn-cert: DFN-CERT-2012-1016
dfn-cert: DFN-CERT-2012-1014
dfn-cert: DFN-CERT-2012-0982
dfn-cert: DFN-CERT-2012-0977
```

[return to 10.0.3.5]

2.1.2 Medium general/tcp

Medium (CVSS: 6.9)
NVT: Ubuntu Update for dbus USN-1576-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1576-1

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable package: libdbus-1-3
Installed version:  1.1.20-1ubuntu1
Fixed version:      1.1.20-1ubuntu3.7
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

dbus on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

Sebastian Krahmer discovered that DBus incorrectly handled environment variables when running with elevated privileges. A local attacker could possibly exploit this flaw with a setuid binary and gain root privileges.

Vulnerability Detection Method

Details: `Ubuntu Update for dbus USN-1576-1`

OID:1.3.6.1.4.1.25623.1.0.841153

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-3524
url: http://www.ubuntu.com/usn/usn-1576-1/
usn: 1576-1
cert-bund: CB-K15/0090
cert-bund: CB-K14/1203
dfn-cert: DFN-CERT-2015-0096
dfn-cert: DFN-CERT-2014-1268
dfn-cert: DFN-CERT-2012-2070
dfn-cert: DFN-CERT-2012-2063
dfn-cert: DFN-CERT-2012-1990
dfn-cert: DFN-CERT-2012-1916
dfn-cert: DFN-CERT-2012-1877
dfn-cert: DFN-CERT-2012-1874
dfn-cert: DFN-CERT-2012-1788
dfn-cert: DFN-CERT-2012-1771
```

Medium (CVSS: 6.9)

NVT: Ubuntu Update for linux vulnerabilities USN-1072-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1072-1

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable package: linux-libc-dev
Installed version:  2.6.24-27.68
Fixed version:      2.6.24-28.86
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
linux vulnerabilities on Ubuntu 8.04 LTS

Vulnerability Insight
Gleb Napatov discovered that KVM did not correctly check certain privileged operations. A local attacker with access to a guest kernel could exploit this to crash the host system, leading to a denial of service. (CVE-2010-0435)
Dave Chinner discovered that the XFS filesystem did not correctly order inode lookups when exported by NFS. A remote attacker could exploit this to read or write disk blocks that had changed file assignment or had become unlinked, leading to a loss of privacy. (CVE-2010-2943)
Dan Rosenberg discovered that several network ioctls did not clear kernel memory correctly. A local user could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-3296, CVE-2010-3297)
Dan Jacobson discovered that ThinkPad video output was not correctly access controlled. A local attacker could exploit this to hang the system, leading to a denial of service. (CVE-2010-3448)
It was discovered that KVM did not correctly initialize certain CPU registers. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-3698)
It was discovered that Xen did not correctly clean up threads. A local attacker in a guest system could exploit this to exhaust host system resources, leading to a denial of service. (CVE-2010-3699)
Brad Spengler discovered that stack memory for new a process was not correctly calculated. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-3858)
Dan Rosenberg discovered that the Linux kernel TIPC implementation contained multiple integer signedness errors. A local attacker could exploit this to gain root privileges. (CVE-2010-3859)
Dan Rosenberg discovered that the Linux kernel X.25 implementation incorrectly parsed facilities. A remote attacker could exploit this to crash the kernel, leading to a denial of service. (CVE-2010-3873)
Vasiliy Kulikov discovered that the Linux kernel X.25 implementation did not correctly clear kernel memory. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-3875)
Vasiliy Kulikov discovered that the Linux kernel sockets implementation did not properly initialize certain structures. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-3876)
Vasiliy Kulikov discovered that the TIPC interface did not correctly initialize certain structures. A local attacker could exploit this to read kernel stack memory, leading to a l ...
Description truncated, please see the referenced URL(s) for more information.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Details: Ubuntu Update for linux vulnerabilities USN-1072-1
OID:1.3.6.1.4.1.25623.1.0.840594
Version used: 2020-08-18T09:42:52Z

References

cve: CVE-2010-0435
cve: CVE-2010-2943
cve: CVE-2010-3296
cve: CVE-2010-3297
cve: CVE-2010-3448
cve: CVE-2010-3698
cve: CVE-2010-3699
cve: CVE-2010-3858
cve: CVE-2010-3859
cve: CVE-2010-3873
cve: CVE-2010-3875
cve: CVE-2010-3876
cve: CVE-2010-3877
cve: CVE-2010-3880
cve: CVE-2010-4072
cve: CVE-2010-4074
cve: CVE-2010-4078
cve: CVE-2010-4079
cve: CVE-2010-4080
cve: CVE-2010-4081
cve: CVE-2010-4083
cve: CVE-2010-4157
cve: CVE-2010-4160
cve: CVE-2010-4248
url: http://www.ubuntu.com/usn/usn-1072-1/
usn: 1072-1
dfn-cert: DFN-CERT-2013-1068
dfn-cert: DFN-CERT-2013-1066
dfn-cert: DFN-CERT-2013-0889
dfn-cert: DFN-CERT-2012-2075
dfn-cert: DFN-CERT-2012-1272
dfn-cert: DFN-CERT-2012-0473
dfn-cert: DFN-CERT-2012-0239
dfn-cert: DFN-CERT-2012-0238
dfn-cert: DFN-CERT-2012-0209
dfn-cert: DFN-CERT-2012-0204
dfn-cert: DFN-CERT-2011-1704
dfn-cert: DFN-CERT-2011-1670
dfn-cert: DFN-CERT-2011-1594
dfn-cert: DFN-CERT-2011-1259
dfn-cert: DFN-CERT-2011-0979
dfn-cert: DFN-CERT-2011-0964

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-0918
dfn-cert: DFN-CERT-2011-0864
dfn-cert: DFN-CERT-2011-0819
dfn-cert: DFN-CERT-2011-0731
dfn-cert: DFN-CERT-2011-0681
dfn-cert: DFN-CERT-2011-0676
dfn-cert: DFN-CERT-2011-0598
dfn-cert: DFN-CERT-2011-0525
dfn-cert: DFN-CERT-2011-0443
dfn-cert: DFN-CERT-2011-0411
dfn-cert: DFN-CERT-2011-0351
dfn-cert: DFN-CERT-2011-0338
dfn-cert: DFN-CERT-2011-0324
dfn-cert: DFN-CERT-2011-0225
dfn-cert: DFN-CERT-2011-0187
dfn-cert: DFN-CERT-2011-0186
dfn-cert: DFN-CERT-2011-0150
dfn-cert: DFN-CERT-2011-0134
dfn-cert: DFN-CERT-2011-0110
dfn-cert: DFN-CERT-2011-0077
dfn-cert: DFN-CERT-2011-0065
dfn-cert: DFN-CERT-2011-0050
dfn-cert: DFN-CERT-2011-0042
dfn-cert: DFN-CERT-2011-0030
dfn-cert: DFN-CERT-2011-0008
dfn-cert: DFN-CERT-2011-0005
dfn-cert: DFN-CERT-2011-0004
dfn-cert: DFN-CERT-2010-1761
dfn-cert: DFN-CERT-2010-1717
dfn-cert: DFN-CERT-2010-1715
dfn-cert: DFN-CERT-2010-1668
dfn-cert: DFN-CERT-2010-1657
dfn-cert: DFN-CERT-2010-1649
dfn-cert: DFN-CERT-2010-1646
dfn-cert: DFN-CERT-2010-1636
dfn-cert: DFN-CERT-2010-1623
dfn-cert: DFN-CERT-2010-1540
dfn-cert: DFN-CERT-2010-1489
dfn-cert: DFN-CERT-2010-1440
dfn-cert: DFN-CERT-2010-1372
dfn-cert: DFN-CERT-2010-1363
dfn-cert: DFN-CERT-2010-1292
dfn-cert: DFN-CERT-2010-1270
dfn-cert: DFN-CERT-2010-1267
dfn-cert: DFN-CERT-2010-1262
dfn-cert: DFN-CERT-2010-1071
```

Medium (CVSS: 6.9)
NVT: Ubuntu Update for dbus USN-1576-2

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1576-2

Vulnerability Detection Result

```
Vulnerable package: libdbus-1-3
Installed version:  1.1.20-1ubuntu1
Fixed version:      1.1.20-1ubuntu3.9
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
dbus on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
USN-1576-1 fixed vulnerabilities in DBus. The update caused a regression for certain services launched from the activation helper, and caused an unclean shutdown on upgrade. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Sebastian Krahmer discovered that DBus incorrectly handled environment variables when running with elevated privileges. A local attacker could possibly exploit this flaw with a setuid binary and gain root privileges.

Vulnerability Detection Method
Details: `Ubuntu Update for dbus USN-1576-2`
OID:1.3.6.1.4.1.25623.1.0.841177
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-3524
url: http://www.ubuntu.com/usn/usn-1576-2/
usn: 1576-2
cert-bund: CB-K15/0090
cert-bund: CB-K14/1203
dfn-cert: DFN-CERT-2015-0096
dfn-cert: DFN-CERT-2014-1268
dfn-cert: DFN-CERT-2012-2070
dfn-cert: DFN-CERT-2012-2063
dfn-cert: DFN-CERT-2012-1990
dfn-cert: DFN-CERT-2012-1916
dfn-cert: DFN-CERT-2012-1877
dfn-cert: DFN-CERT-2012-1874
dfn-cert: DFN-CERT-2012-1788
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-1771
```

Medium (CVSS: 6.9)
NVT: Ubuntu Update for pam USN-1237-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1237-1

Vulnerability Detection Result

```
Vulnerable package: libpam-modules
Installed version:  0.99.7.1-5ubuntu6
Fixed version:      0.99.7.1-5ubuntu6.5
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
pam on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Kees Cook discovered that the PAM pam_env module incorrectly handled certain malformed environment files. A local attacker could use this flaw to cause a denial of service, or possibly gain privileges. The default compiler options for affected releases should reduce the vulnerability to a denial of service. (CVE-2011-3148)
Kees Cook discovered that the PAM pam_env module incorrectly handled variable expansion. A local attacker could use this flaw to cause a denial of service. (CVE-2011-3149)
Stephane Chazelas discovered that the PAM pam_motd module incorrectly cleaned the environment during execution of the motd scripts. In certain environments, a local attacker could use this to execute arbitrary code as root, and gain privileges.

Vulnerability Detection Method
Details: `Ubuntu Update for pam USN-1237-1`
OID:1.3.6.1.4.1.25623.1.0.840794
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-3148
cve: CVE-2011-3149
cve: CVE-2011-3628
url: http://www.ubuntu.com/usn/usn-1237-1/
usn: 1237-1
dfn-cert: DFN-CERT-2013-0341
dfn-cert: DFN-CERT-2011-1879
dfn-cert: DFN-CERT-2011-1833
dfn-cert: DFN-CERT-2011-1699
dfn-cert: DFN-CERT-2011-1687
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-1684
dfn-cert: DFN-CERT-2011-1649
```

Medium (CVSS: 6.9)
NVT: Ubuntu Update for postfix USN-1113-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1113-1

Vulnerability Detection Result

```
Vulnerable package: postfix
Installed version:  2.5.1-2ubuntu1
Fixed version:      2.5.1-2ubuntu1.3
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
postfix on Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 9.10, Ubuntu 8.04 LTS, Ubuntu 6.06 LTS

Vulnerability Insight
It was discovered that the Postfix package incorrectly granted write access on the PID directory to the postfix user. A local attacker could use this flaw to possibly conduct a symlink attack and overwrite arbitrary files. This issue only affected Ubuntu 6.06 LTS and 8.04 LTS. (CVE-2009-2939)
Wietse Venema discovered that Postfix incorrectly handled cleartext commands after TLS is in place. A remote attacker could exploit this to inject cleartext commands into TLS sessions, and possibly obtain confidential information such as passwords. (CVE-2011-0411)

Vulnerability Detection Method
Details: `Ubuntu Update for postfix USN-1113-1`
OID:1.3.6.1.4.1.25623.1.0.840648
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2009-2939
cve: CVE-2011-0411
url: http://www.ubuntu.com/usn/usn-1113-1/
usn: 1113-1
cert-bund: CB-K15/1514
dfn-cert: DFN-CERT-2011-0844
dfn-cert: DFN-CERT-2011-0771
dfn-cert: DFN-CERT-2011-0741
dfn-cert: DFN-CERT-2011-0712
dfn-cert: DFN-CERT-2011-0673
dfn-cert: DFN-CERT-2011-0597
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-0596
dfn-cert: DFN-CERT-2011-0519
dfn-cert: DFN-CERT-2011-0516
dfn-cert: DFN-CERT-2011-0483
dfn-cert: DFN-CERT-2011-0434
dfn-cert: DFN-CERT-2011-0393
dfn-cert: DFN-CERT-2011-0381
```

Medium (CVSS: 6.9)
NVT: Ubuntu Update for pam USN-1140-2

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1140-2

Vulnerability Detection Result

```
Vulnerable package: libpam-modules
Installed version:  0.99.7.1-5ubuntu6
Fixed version:      0.99.7.1-5ubuntu6.4
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
pam on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
USN-1140-1 fixed vulnerabilities in PAM. A regression was found that caused cron to stop working with a 'Module is unknown' error. As a result, systems configured with automatic updates will not receive updates until cron is restarted, these updates are installed or the system is rebooted. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Marcus Granado discovered that PAM incorrectly handled configuration files with non-ASCII usernames. A remote attacker could use this flaw to cause a denial of service, or possibly obtain login access with a different users username. This issue only affected Ubuntu 8.04 LTS. (CVE-2009-0887)
It was discovered that the PAM pam_xauth, pam_env and pam_mail modules incorrectly handled dropping privileges when performing operations. A local attacker could use this flaw to read certain arbitrary files, and access other sensitive information. (CVE-2010-3316, CVE-2010-3430, CVE-2010-3431, CVE-2010-3435)
It was discovered that the PAM pam_namespace module incorrectly cleaned the environment during execution of the namespace.init script. A local attacker could use this flaw to possibly gain privileges. (CVE-2010-3853)
It was discovered that the PAM pam_xauth module incorrectly handled certain failures. A local attacker could use this flaw to delete certain unintended files. (CVE-2010-4706)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that the PAM pam_xauth module incorrectly verified certain file properties. A local attacker could use this flaw to cause a denial of service. (CVE-2010-4707)

Vulnerability Detection Method
Details: `Ubuntu Update for pam USN-1140-2`
OID:1.3.6.1.4.1.25623.1.0.840673
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2009-0887
cve: CVE-2010-3316
cve: CVE-2010-3430
cve: CVE-2010-3431
cve: CVE-2010-3435
cve: CVE-2010-3853
cve: CVE-2010-4706
cve: CVE-2010-4707
url: http://www.ubuntu.com/usn/usn-1140-2/
usn: 1140-2
dfn-cert: DFN-CERT-2011-1699
dfn-cert: DFN-CERT-2011-1684
dfn-cert: DFN-CERT-2011-0325
dfn-cert: DFN-CERT-2010-1583
dfn-cert: DFN-CERT-2010-1574
dfn-cert: DFN-CERT-2010-1506
dfn-cert: DFN-CERT-2010-1495
dfn-cert: DFN-CERT-2010-1494
dfn-cert: DFN-CERT-2010-1476
```

Medium (CVSS: 6.9)
NVT: Ubuntu Update for pam USN-1140-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1140-1

Vulnerability Detection Result

```
Vulnerable package: libpam-modules
Installed version:  0.99.7.1-5ubuntu6
Fixed version:      0.99.7.1-5ubuntu6.3
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
pam on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Marcus Granado discovered that PAM incorrectly handled configuration files with non-ASCII usernames. A remote attacker could use this flaw to cause a denial of service, or possibly obtain login access with a different users username. This issue only affected Ubuntu 8.04 LTS. (CVE-2009-0887)

It was discovered that the PAM pam_xauth, pam_env and pam_mail modules incorrectly handled dropping privileges when performing operations. A local attacker could use this flaw to read certain arbitrary files, and access other sensitive information. (CVE-2010-3316, CVE-2010-3430, CVE-2010-3431, CVE-2010-3435)

It was discovered that the PAM pam_namespace module incorrectly cleaned the environment during execution of the namespace.init script. A local attacker could use this flaw to possibly gain privileges. (CVE-2010-3853)

It was discovered that the PAM pam_xauth module incorrectly handled certain failures. A local attacker could use this flaw to delete certain unintended files. (CVE-2010-4706)

It was discovered that the PAM pam_xauth module incorrectly verified certain file properties. A local attacker could use this flaw to cause a denial of service. (CVE-2010-4707)

Vulnerability Detection Method

Details: `Ubuntu Update for pam USN-1140-1`
OID:1.3.6.1.4.1.25623.1.0.840672
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2009-0887
cve: CVE-2010-3316
cve: CVE-2010-3430
cve: CVE-2010-3431
cve: CVE-2010-3435
cve: CVE-2010-3853
cve: CVE-2010-4706
cve: CVE-2010-4707
url: http://www.ubuntu.com/usn/usn-1140-1/
usn: 1140-1
dfn-cert: DFN-CERT-2011-1699
dfn-cert: DFN-CERT-2011-1684
dfn-cert: DFN-CERT-2011-0325
dfn-cert: DFN-CERT-2010-1583
dfn-cert: DFN-CERT-2010-1574
dfn-cert: DFN-CERT-2010-1506
dfn-cert: DFN-CERT-2010-1495
dfn-cert: DFN-CERT-2010-1494
dfn-cert: DFN-CERT-2010-1476
```

Medium (CVSS: 6.9)
NVT: Ubuntu Update for logrotate USN-1172-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1172-1

Vulnerability Detection Result

```
Vulnerable package: logrotate
Installed version:  3.7.1-3
Fixed version:      3.7.1-3ubuntu0.8.04.1
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

logrotate on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

It was discovered that logrotate incorrectly handled the creation of new log files. Local users could possibly read log files if they were opened before permissions were in place. This issue only affected Ubuntu 8.04 LTS. (CVE-2011-1098)
It was discovered that logrotate incorrectly handled certain log file names when used with the shred option. Local attackers able to create log files with specially crafted filenames could use this issue to execute arbitrary code. This issue only affected Ubuntu 10.04 LTS, 10.10, and 11.04. (CVE-2011-1154)
It was discovered that logrotate incorrectly handled certain malformed log filenames. Local attackers able to create log files with specially crafted filenames could use this issue to cause logrotate to stop processing log files, resulting in a denial of service. (CVE-2011-1155)
It was discovered that logrotate incorrectly handled symlinks and hard links when processing log files. A local attacker having write access to a log file directory could use this issue to overwrite or read arbitrary files. This issue only affected Ubuntu 8.04 LTS. (CVE-2011-1548)

Vulnerability Detection Method

Details: `Ubuntu Update for logrotate USN-1172-1`
OID:1.3.6.1.4.1.25623.1.0.840705
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-1098
cve: CVE-2011-1154
cve: CVE-2011-1155
cve: CVE-2011-1548
url: http://www.ubuntu.com/usn/usn-1172-1/
usn: 1172-1
cert-bund: CB-K15/0957
dfn-cert: DFN-CERT-2015-1003
dfn-cert: DFN-CERT-2011-0844
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-0543
dfn-cert: DFN-CERT-2011-0512
dfn-cert: DFN-CERT-2011-0480
dfn-cert: DFN-CERT-2011-0462
```

Medium (CVSS: 6.9)
NVT: Ubuntu Update for python2.5 USN-1613-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1613-1

Vulnerability Detection Result

```
Vulnerable package: python2.5
Installed version:  2.5.2-2ubuntu6.1
Fixed version:      2.5.2-2ubuntu6.2
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
python2.5 on Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that Python would prepend an empty string to sys.path under certain circumstances. A local attacker with write access to the current working directory could exploit this to execute arbitrary code. (CVE-2008-5983)
It was discovered that the audioop module did not correctly perform input validation. If a user or automatated system were tricked into opening a crafted audio file, an attacker could cause a denial of service via application crash. (CVE-2010-1634, CVE-2010-2089)
Giampaolo Rodola discovered several race conditions in the smtpd module. A remote attacker could exploit this to cause a denial of service via daemon outage. (CVE-2010-3493)
It was discovered that the CGIHTTPServer module did not properly perform input validation on certain HTTP GET requests. A remote attacker could potentially obtain access to CGI script source files. (CVE-2011-1015)
Niels Heinen discovered that the urllib and urllib2 modules would process Location headers that specify a redirection to file: URLs. A remote attacker could exploit this to obtain sensitive information or cause a denial of service. (CVE-2011-1521)
It was discovered that SimpleHTTPServer did not use a charset parameter in the Content-Type HTTP header. An attacker could potentially exploit this to conduct cross-site scripting (XSS) attacks against Internet Explorer 7 users. (CVE-2011-4940)
It was discovered that Python distutils contained a race condition when creating the /.pypirc file. A local attacker could exploit this to obtain sensitive information. (CVE-2011-4944)
It was discovered that SimpleXMLRPCServer did not properly validate its input when handling HTTP POST requests. A remote attacker could exploit this to cause a denial of service via excessive CPU utilization. (CVE-2012-0845)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that the Expat module in Python 2.5 computed hash values without restricting the ability to trigger hash collisions predictably. If a user or application using pyexpat were tricked into opening a crafted XML file, an attacker could cause a denial of service by consuming excessive CPU resources. (CVE-2012-0876)

Tim Boddy discovered that the Expat module in Python 2.5 did not properly handle memory reallocation when processing XML files. If a user or application using pyexpat were tricked into opening a crafted XML file, an attacker could cause a denial of service by consuming excessive memory resources. (CVE-2012-1148)

Vulnerability Detection Method

Details: `Ubuntu Update for python2.5 USN-1613-1`
OID:1.3.6.1.4.1.25623.1.0.841195
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2008-5983
cve: CVE-2010-1634
cve: CVE-2010-2089
cve: CVE-2010-3493
cve: CVE-2011-1015
cve: CVE-2011-1521
cve: CVE-2011-4940
cve: CVE-2011-4944
cve: CVE-2012-0845
cve: CVE-2012-0876
cve: CVE-2012-1148
url: http://www.ubuntu.com/usn/usn-1613-1/
usn: 1613-1
cert-bund: CB-K17/0536
cert-bund: CB-K17/0492
cert-bund: CB-K16/1972
cert-bund: CB-K16/1816
cert-bund: CB-K16/0112
cert-bund: CB-K15/1792
cert-bund: CB-K15/0987
cert-bund: CB-K13/0845
dfn-cert: DFN-CERT-2020-0405
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2017-0551
dfn-cert: DFN-CERT-2017-0508
dfn-cert: DFN-CERT-2016-2081
dfn-cert: DFN-CERT-2016-1923
dfn-cert: DFN-CERT-2016-0125
dfn-cert: DFN-CERT-2015-1898
dfn-cert: DFN-CERT-2015-1035
dfn-cert: DFN-CERT-2013-1847
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-2129
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1522
dfn-cert: DFN-CERT-2012-1513
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1169
dfn-cert: DFN-CERT-2012-1168
dfn-cert: DFN-CERT-2012-1133
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0948
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0835
dfn-cert: DFN-CERT-2012-0693
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0567
dfn-cert: DFN-CERT-2012-0559
dfn-cert: DFN-CERT-2012-0171
dfn-cert: DFN-CERT-2011-1533
dfn-cert: DFN-CERT-2011-1500
dfn-cert: DFN-CERT-2011-1436
dfn-cert: DFN-CERT-2011-0844
dfn-cert: DFN-CERT-2011-0801
dfn-cert: DFN-CERT-2011-0789
dfn-cert: DFN-CERT-2011-0771
dfn-cert: DFN-CERT-2011-0723
dfn-cert: DFN-CERT-2011-0718
dfn-cert: DFN-CERT-2011-0111
dfn-cert: DFN-CERT-2011-0051
dfn-cert: DFN-CERT-2010-1762
dfn-cert: DFN-CERT-2010-1482
dfn-cert: DFN-CERT-2010-1469
dfn-cert: DFN-CERT-2010-1156
dfn-cert: DFN-CERT-2010-0901
dfn-cert: DFN-CERT-2010-0857
dfn-cert: DFN-CERT-2010-0782
```

Medium (CVSS: 6.9)
NVT: Ubuntu Update for sudo USN-1754-1

Summary

. . . continues on next page . . .

... continued from previous page ...

The remote host is missing an update for the 'sudo' package(s) announced via the referenced advisory.

Vulnerability Detection Result

```
Vulnerable package: sudo
Installed version:  1.6.9p10-1ubuntu3
Fixed version:      1.6.9p10-1ubuntu3.10
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

sudo on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

Marco Schoepl discovered that Sudo incorrectly handled time stamp files when the system clock is set to epoch. A local attacker could use this issue to run Sudo commands without a password prompt.

Vulnerability Detection Method

Details: `Ubuntu Update for sudo USN-1754-1`

OID:1.3.6.1.4.1.25623.1.0.841349

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2013-1775
url: http://www.ubuntu.com/usn/usn-1754-1/
usn: 1754-1
cert-bund: CB-K16/1107
cert-bund: CB-K15/1188
cert-bund: CB-K13/0849
cert-bund: CB-K13/0735
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2015-1252
dfn-cert: DFN-CERT-2013-1856
dfn-cert: DFN-CERT-2013-1725
dfn-cert: DFN-CERT-2013-1109
dfn-cert: DFN-CERT-2013-0944
dfn-cert: DFN-CERT-2013-0615
dfn-cert: DFN-CERT-2013-0610
dfn-cert: DFN-CERT-2013-0600
dfn-cert: DFN-CERT-2013-0580
dfn-cert: DFN-CERT-2013-0519
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for tiff USN-1416-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1416-1

Vulnerability Detection Result

```
Vulnerable package: libtiff4
Installed version:  3.8.2-7ubuntu3.4
Fixed version:      3.8.2-7ubuntu3.10
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
tiff on Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Alexander Gavrun discovered that the TIFF library incorrectly allocated space for a tile. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could execute arbitrary code with user privileges, or crash the application, leading to a denial of service. (CVE-2012-1173)
It was discovered that the tiffdump utility incorrectly handled directory data structures with many directory entries. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. This issue only applied to Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2010-4665)

Vulnerability Detection Method
Details: `Ubuntu Update for tiff USN-1416-1`
OID:1.3.6.1.4.1.25623.1.0.840976
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-1173
cve: CVE-2010-4665
url: http://www.ubuntu.com/usn/usn-1416-1/
usn: 1416-1
cert-bund: CB-K13/0930
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2013-1950
dfn-cert: DFN-CERT-2012-1879
dfn-cert: DFN-CERT-2012-1255
dfn-cert: DFN-CERT-2012-0763
dfn-cert: DFN-CERT-2012-0760
dfn-cert: DFN-CERT-2012-0755
dfn-cert: DFN-CERT-2012-0674
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0663
dfn-cert: DFN-CERT-2012-0631
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0624
dfn-cert: DFN-CERT-2011-0771
dfn-cert: DFN-CERT-2011-0712
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for libxml2 USN-1587-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1587-1

Vulnerability Detection Result

```
Vulnerable package: libxml2
Installed version:  2.6.31.dfsg-2ubuntu1
Fixed version:      2.6.31.dfsg-2ubuntu1.10
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
libxml2 on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Juri Aedla discovered that libxml2 incorrectly handled certain memory operations. If a user or application linked against libxml2 were tricked into opening a specially crafted XML file, an attacker could cause the application to crash or possibly execute arbitrary code with the privileges of the user invoking the program.

Vulnerability Detection Method
Details: `Ubuntu Update for libxml2 USN-1587-1`
OID:1.3.6.1.4.1.25623.1.0.841166
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-2807
url: http://www.ubuntu.com/usn/usn-1587-1/
usn: 1587-1
cert-bund: CB-K14/0091
cert-bund: CB-K13/0874
cert-bund: CB-K13/0834
dfn-cert: DFN-CERT-2014-0093
dfn-cert: DFN-CERT-2013-1307
dfn-cert: DFN-CERT-2013-0199
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-1873
dfn-cert: DFN-CERT-2012-1841
dfn-cert: DFN-CERT-2012-1539
dfn-cert: DFN-CERT-2012-1524
dfn-cert: DFN-CERT-2012-1498
dfn-cert: DFN-CERT-2012-1299
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for libpng USN-1175-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1175-1

Vulnerability Detection Result

```
Vulnerable package: libpng12-0
Installed version:  1.2.15~beta5-3ubuntu0.2
Fixed version:      1.2.15~beta5-3ubuntu0.4
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
libpng on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Frank Busse discovered that libpng did not properly handle certain malformed PNG images. If a user or automated system were tricked into opening a crafted PNG file, an attacker could cause libpng to crash, resulting in a denial of service. This issue only affected Ubuntu 10.04 LTS, 10.10, and 11.04. (CVE-2011-2501)
It was discovered that libpng did not properly handle certain malformed PNG images. If a user or automated system were tricked into opening a crafted PNG file, an attacker could cause a denial of service or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-2690)
Frank Busse discovered that libpng did not properly handle certain PNG images with invalid sCAL chunks. If a user or automated system were tricked into opening a crafted PNG file, an attacker could cause a denial of service or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-2692)

Vulnerability Detection Method
Details: `Ubuntu Update for libpng USN-1175-1`
OID:1.3.6.1.4.1.25623.1.0.840714
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-2501
cve: CVE-2011-2690
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2011-2692
url: http://www.ubuntu.com/usn/usn-1175-1/
usn: 1175-1
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2011-1607
dfn-cert: DFN-CERT-2011-1290
dfn-cert: DFN-CERT-2011-1149
dfn-cert: DFN-CERT-2011-1146
dfn-cert: DFN-CERT-2011-1145
dfn-cert: DFN-CERT-2011-1144
dfn-cert: DFN-CERT-2011-1143
dfn-cert: DFN-CERT-2011-1105
dfn-cert: DFN-CERT-2011-1085
dfn-cert: DFN-CERT-2011-1070
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for libpng USN-1367-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1367-1

Vulnerability Detection Result

```
Vulnerable package: libpng12-0
Installed version:  1.2.15~beta5-3ubuntu0.2
Fixed version:      1.2.15~beta5-3ubuntu0.5
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
libpng on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that libpng did not properly verify the embedded profile length of iCCP chunks. An attacker could exploit this to cause a denial of service via application crash. This issue only affected Ubuntu 8.04 LTS. (CVE-2009-5063)
Jueri Aedla discovered that libpng did not properly verify the size used when allocating memory during chunk decompression. If a user or automated system using libpng were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service or execute code with the privileges of the user invoking the program. (CVE-2011-3026)

Vulnerability Detection Method
Details: `Ubuntu Update for libpng USN-1367-1`
OID:1.3.6.1.4.1.25623.1.0.840897
Version used: `2020-04-21T06:28:23Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2009-5063
cve: CVE-2011-3026
url: http://www.ubuntu.com/usn/usn-1367-1/
usn: 1367-1
dfn-cert: DFN-CERT-2012-1531
dfn-cert: DFN-CERT-2012-0680
dfn-cert: DFN-CERT-2012-0639
dfn-cert: DFN-CERT-2012-0599
dfn-cert: DFN-CERT-2012-0421
dfn-cert: DFN-CERT-2012-0410
dfn-cert: DFN-CERT-2012-0409
dfn-cert: DFN-CERT-2012-0391
dfn-cert: DFN-CERT-2012-0388
dfn-cert: DFN-CERT-2012-0378
dfn-cert: DFN-CERT-2012-0376
dfn-cert: DFN-CERT-2012-0375
dfn-cert: DFN-CERT-2012-0367
dfn-cert: DFN-CERT-2012-0364
dfn-cert: DFN-CERT-2012-0363
dfn-cert: DFN-CERT-2012-0355
dfn-cert: DFN-CERT-2012-0353
dfn-cert: DFN-CERT-2012-0341
dfn-cert: DFN-CERT-2012-0316
dfn-cert: DFN-CERT-2012-0315
dfn-cert: DFN-CERT-2012-0307
dfn-cert: DFN-CERT-2012-0295
dfn-cert: DFN-CERT-2012-0289
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for libxml2 USN-1656-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1656-1

Vulnerability Detection Result

```
Vulnerable package: libxml2
Installed version:  2.6.31.dfsg-2ubuntu1
Fixed version:      2.6.31.dfsg-2ubuntu1.11
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

libxml2 on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

It was discovered that libxml2 had a heap-based buffer underflow when parsing entities. If a user or automated system were tricked into processing a specially crafted XML document, applications linked against libxml2 could be made to crash or possibly execute arbitrary code.

Vulnerability Detection Method

Details: `Ubuntu Update for libxml2 USN-1656-1`
OID:1.3.6.1.4.1.25623.1.0.841242
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-5134
url: http://www.ubuntu.com/usn/usn-1656-1/
usn: 1656-1
cert-bund: CB-K15/0050
cert-bund: CB-K14/0091
cert-bund: CB-K13/0874
cert-bund: CB-K13/0834
dfn-cert: DFN-CERT-2015-0049
dfn-cert: DFN-CERT-2014-0093
dfn-cert: DFN-CERT-2013-1230
dfn-cert: DFN-CERT-2013-1046
dfn-cert: DFN-CERT-2013-0944
dfn-cert: DFN-CERT-2013-0688
dfn-cert: DFN-CERT-2013-0196
dfn-cert: DFN-CERT-2013-0138
dfn-cert: DFN-CERT-2012-2265
dfn-cert: DFN-CERT-2012-2251
dfn-cert: DFN-CERT-2012-2246
dfn-cert: DFN-CERT-2012-2195
dfn-cert: DFN-CERT-2012-2190
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for postgresql-9.1 USN-1717-1

Summary

The remote host is missing an update for the 'postgresql-9.1' package(s) announced via the referenced advisory.

Vulnerability Detection Result

```
Vulnerable package: postgresql-8.3
Installed version:  8.3.1-1
Fixed version:      8.3.23-0ubuntu8.04
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
postgresql-9.1 on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Sumit Soni discovered that PostgreSQL incorrectly handled calling a certain internal function with invalid arguments. An authenticated attacker could use this issue to cause PostgreSQL to crash, resulting in a denial of service.

Vulnerability Detection Method
Details: `Ubuntu Update for postgresql-9.1 USN-1717-1`
OID:1.3.6.1.4.1.25623.1.0.841317
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2013-0255
url: http://www.ubuntu.com/usn/usn-1717-1/
usn: 1717-1
cert-bund: CB-K13/0851
dfn-cert: DFN-CERT-2013-1861
dfn-cert: DFN-CERT-2013-0723
dfn-cert: DFN-CERT-2013-0376
dfn-cert: DFN-CERT-2013-0355
dfn-cert: DFN-CERT-2013-0322
dfn-cert: DFN-CERT-2013-0251
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for libpng USN-1402-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1402-1

Vulnerability Detection Result

```
Vulnerable package: libpng12-0
Installed version:  1.2.15~beta5-3ubuntu0.2
Fixed version:      1.2.15~beta5-3ubuntu0.6
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

libpng on Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

It was discovered that libpng did not properly process compressed chunks. If a user or automated system using libpng were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service or execute code with the privileges of the user invoking the program.

Vulnerability Detection Method

Details: `Ubuntu Update for libpng USN-1402-1`

OID:1.3.6.1.4.1.25623.1.0.840960

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-3045
url: http://www.ubuntu.com/usn/usn-1402-1/
usn: 1402-1
dfn-cert: DFN-CERT-2012-0625
dfn-cert: DFN-CERT-2012-0598
dfn-cert: DFN-CERT-2012-0597
dfn-cert: DFN-CERT-2012-0539
dfn-cert: DFN-CERT-2012-0526
dfn-cert: DFN-CERT-2012-0518
dfn-cert: DFN-CERT-2012-0515
dfn-cert: DFN-CERT-2012-0499
dfn-cert: DFN-CERT-2012-0479
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for postgresql-9.1 USN-1378-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1378-1

Vulnerability Detection Result

```
Vulnerable package: postgresql-8.3
Installed version:  8.3.1-1
Fixed version:      8.3.18-0ubuntu0.8.04
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

postgresql-9.1 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

It was discovered that PostgreSQL incorrectly checked permissions on functions called by a trigger. An attacker could attach a trigger to a table they owned and possibly escalate privileges. (CVE-2012-0866)

It was discovered that PostgreSQL incorrectly truncated SSL certificate name checks to 32 characters. If a host name was exactly 32 characters, this issue could be exploited by an attacker to spoof the SSL certificate. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, Ubuntu 11.04 and Ubuntu 11.10. (CVE-2012-0867)

It was discovered that the PostgreSQL pg_dump utility incorrectly filtered line breaks in object names. An attacker could create object names that execute arbitrary SQL commands when a dump script is reloaded. (CVE-2012-0868)

Vulnerability Detection Method

Details: `Ubuntu Update for postgresql-9.1 USN-1378-1`
OID:1.3.6.1.4.1.25623.1.0.840921
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-0866
cve: CVE-2012-0867
cve: CVE-2012-0868
url: http://www.ubuntu.com/usn/usn-1378-1/
usn: 1378-1
cert-bund: CB-K15/1514
dfn-cert: DFN-CERT-2012-1782
dfn-cert: DFN-CERT-2012-0973
dfn-cert: DFN-CERT-2012-0972
dfn-cert: DFN-CERT-2012-0854
dfn-cert: DFN-CERT-2012-0678
dfn-cert: DFN-CERT-2012-0437
dfn-cert: DFN-CERT-2012-0427
dfn-cert: DFN-CERT-2012-0397
dfn-cert: DFN-CERT-2012-0393
dfn-cert: DFN-CERT-2012-0386
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for postfix USN-1131-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1131-1

Vulnerability Detection Result

```
Vulnerable package: postfix
Installed version:  2.5.1-2ubuntu1
Fixed version:      2.5.1-2ubuntu1.4
```

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
postfix on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS, Ubuntu 6.06 LTS

Vulnerability Insight
Thomas Jarosch discovered that Postfix incorrectly handled authentication mechanisms other than PLAIN and LOGIN when the Cyrus SASL library is used. A remote attacker could use this to cause Postfix to crash, leading to a denial of service, or possibly execute arbitrary code as the postfix user.

Vulnerability Detection Method
Details: `Ubuntu Update for postfix USN-1131-1`
OID:1.3.6.1.4.1.25623.1.0.840658
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-1720
url: http://www.ubuntu.com/usn/usn-1131-1/
usn: 1131-1
cert-bund: CB-K15/1514
dfn-cert: DFN-CERT-2011-0849
dfn-cert: DFN-CERT-2011-0844
dfn-cert: DFN-CERT-2011-0780
dfn-cert: DFN-CERT-2011-0772
dfn-cert: DFN-CERT-2011-0770
dfn-cert: DFN-CERT-2011-0744
dfn-cert: DFN-CERT-2011-0741
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for php5 vulnerabilities USN-1042-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1042-1

Vulnerability Detection Result

```
Vulnerable package: php5-cgi
Installed version:  5.2.4-2ubuntu5.10
Fixed version:      5.2.4-2ubuntu5.13
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

php5 vulnerabilities on Ubuntu 6.06 LTS, Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight

It was discovered that an integer overflow in the XML UTF-8 decoding code could allow an attacker to bypass cross-site scripting (XSS) protections. This issue only affected Ubuntu 6.06 LTS, Ubuntu 8.04 LTS, and Ubuntu 9.10. (CVE-2009-5016)

It was discovered that the XML UTF-8 decoding code did not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which could allow an attacker to bypass cross-site scripting (XSS) protections. (CVE-2010-3870)

It was discovered that attackers might be able to bypass open_basedir() restrictions by passing a specially crafted filename. (CVE-2010-3436)

Maksymilian Arciemowicz discovered that a NULL pointer dereference in the ZIP archive handling code could allow an attacker to cause a denial of service through a specially crafted ZIP archive. This issue only affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, and Ubuntu 10.10. (CVE-2010-3709)

It was discovered that a stack consumption vulnerability in the filter_var() PHP function when in FILTER_VALIDATE_EMAIL mode, could allow a remote attacker to cause a denial of service. This issue only affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, and Ubuntu 10.10. (CVE-2010-3710)

It was discovered that the mb_strcut function in the Libmbfl library within PHP could allow an attacker to read arbitrary memory within the application process. This issue only affected Ubuntu 10.10. (CVE-2010-4156)

Maksymilian Arciemowicz discovered that an integer overflow in the NumberFormatter::getSymbol function could allow an attacker to cause a denial of service. This issue only affected Ubuntu 10.04 LTS and Ubuntu 10.10. (CVE-2010-4409)

Rick Regan discovered that when handing PHP textual representations of the largest subnormal double-precision floating-point number, the zend_strtod function could go into an infinite loop on 32bit x86 processors, allowing an attacker to cause a denial of service. (CVE-2010-4645)

Vulnerability Detection Method

Details: `Ubuntu Update for php5 vulnerabilities USN-1042-1`

OID:1.3.6.1.4.1.25623.1.0.840564

Version used: `2019-09-16T06:54:58Z`

References

```
cve: CVE-2009-5016
cve: CVE-2010-3436
cve: CVE-2010-3709
cve: CVE-2010-3710
cve: CVE-2010-3870
cve: CVE-2010-4156
cve: CVE-2010-4409
cve: CVE-2010-4645
url: http://www.ubuntu.com/usn/usn-1042-1/
usn: 1042-1
dfn-cert: DFN-CERT-2012-0731
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0514
dfn-cert: DFN-CERT-2012-0109
dfn-cert: DFN-CERT-2011-0642
dfn-cert: DFN-CERT-2011-0515
dfn-cert: DFN-CERT-2011-0445
dfn-cert: DFN-CERT-2011-0432
dfn-cert: DFN-CERT-2011-0402
dfn-cert: DFN-CERT-2011-0148
dfn-cert: DFN-CERT-2011-0147
dfn-cert: DFN-CERT-2011-0097
dfn-cert: DFN-CERT-2011-0096
dfn-cert: DFN-CERT-2011-0095
dfn-cert: DFN-CERT-2011-0013
dfn-cert: DFN-CERT-2011-0012
dfn-cert: DFN-CERT-2011-0011
dfn-cert: DFN-CERT-2010-1729
dfn-cert: DFN-CERT-2010-1706
dfn-cert: DFN-CERT-2010-1664
dfn-cert: DFN-CERT-2010-1620
dfn-cert: DFN-CERT-2010-1530
dfn-cert: DFN-CERT-2010-1526
dfn-cert: DFN-CERT-2010-1471
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for tiff vulnerability USN-1102-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1102-1

Vulnerability Detection Result

```
Vulnerable package: libtiff4
Installed version:  3.8.2-7ubuntu3.4
Fixed version:      3.8.2-7ubuntu3.9
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
tiff vulnerability on Ubuntu 6.06 LTS, Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Martin Barbella discovered that the thunder (aka ThunderScan) decoder in the TIFF library incorrectly handled an unexpected BitsPerSample value. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could execute arbitrary code with user privileges, or crash the application, leading to a denial of service.

Vulnerability Detection Method

Details: `Ubuntu Update for tiff vulnerability USN-1102-1`
OID:1.3.6.1.4.1.25623.1.0.840626
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-1167
url: http://www.ubuntu.com/usn/usn-1102-1/
usn: 1102-1
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2011-0771
dfn-cert: DFN-CERT-2011-0713
dfn-cert: DFN-CERT-2011-0712
dfn-cert: DFN-CERT-2011-0694
dfn-cert: DFN-CERT-2011-0667
dfn-cert: DFN-CERT-2011-0541
dfn-cert: DFN-CERT-2011-0537
dfn-cert: DFN-CERT-2011-0503
dfn-cert: DFN-CERT-2011-0493
dfn-cert: DFN-CERT-2011-0455
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for tiff USN-1655-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1655-1

Vulnerability Detection Result

```
Vulnerable package: libtiff4
Installed version:  3.8.2-7ubuntu3.4
Fixed version:      3.8.2-7ubuntu3.16
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

tiff on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that LibTIFF incorrectly handled certain malformed images using the DOTRANGE tag. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges.

Vulnerability Detection Method

Details: `Ubuntu Update for tiff USN-1655-1`
OID:1.3.6.1.4.1.25623.1.0.841244
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-5581
url: http://www.ubuntu.com/usn/usn-1655-1/
usn: 1655-1
cert-bund: CB-K13/0930
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2013-1950
dfn-cert: DFN-CERT-2013-0154
dfn-cert: DFN-CERT-2013-0006
dfn-cert: DFN-CERT-2012-2274
dfn-cert: DFN-CERT-2012-2267
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for openldap, openldap2.3 vulnerabilities USN-1100-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1100-1

Vulnerability Detection Result

```
Vulnerable package: libldap-2.4-2
Installed version:  2.4.9-0ubuntu0.8.04.3
Fixed version:      2.4.9-0ubuntu0.8.04.5
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

openldap, openldap2.3 vulnerabilities on Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight

It was discovered that OpenLDAP did not properly check forwarded authentication failures when using a slave server and chain overlay. If OpenLDAP were configured in this manner, an attacker could bypass authentication checks by sending an invalid password to a slave server. (CVE-2011-1024)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that OpenLDAP did not properly perform authentication checks to the rootdn when using the back-ndb backend. An attacker could exploit this to access the directory by sending an arbitrary password. Ubuntu does not ship OpenLDAP with back-ndb support by default. This issue did not affect Ubuntu 8.04 LTS. (CVE-2011-1025)
It was discovered that OpenLDAP did not properly validate modrdn requests. An unauthenticated remote user could use this to cause a denial of service via application crash. (CVE-2011-1081)

Vulnerability Detection Method
Details: `Ubuntu Update for openldap, openldap2.3 vulnerabilities USN-1100-1`
OID:1.3.6.1.4.1.25623.1.0.840624
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-1024
cve: CVE-2011-1025
cve: CVE-2011-1081
url: http://www.ubuntu.com/usn/usn-1100-1/
usn: 1100-1
cert-bund: CB-K16/0564
cert-bund: CB-K15/1514
dfn-cert: DFN-CERT-2011-1466
dfn-cert: DFN-CERT-2011-0634
dfn-cert: DFN-CERT-2011-0608
dfn-cert: DFN-CERT-2011-0471
dfn-cert: DFN-CERT-2011-0470
dfn-cert: DFN-CERT-2011-0355
dfn-cert: DFN-CERT-2011-0354
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for libpng USN-1417-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1417-1

Vulnerability Detection Result

```
Vulnerable package: libpng12-0
Installed version:  1.2.15~beta5-3ubuntu0.2
Fixed version:      1.2.15~beta5-3ubuntu0.7
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
libpng on Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

It was discovered that libpng incorrectly handled certain memory operations. If a user or automated system using libpng were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service or execute code with the privileges of the user invoking the program.

Vulnerability Detection Method

Details: `Ubuntu Update for libpng USN-1417-1`
OID:1.3.6.1.4.1.25623.1.0.840979
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-3048
url: http://www.ubuntu.com/usn/usn-1417-1/
usn: 1417-1
cert-bund: CB-K14/1476
dfn-cert: DFN-CERT-2014-1559
dfn-cert: DFN-CERT-2012-1531
dfn-cert: DFN-CERT-2012-0800
dfn-cert: DFN-CERT-2012-0787
dfn-cert: DFN-CERT-2012-0702
dfn-cert: DFN-CERT-2012-0668
dfn-cert: DFN-CERT-2012-0634
dfn-cert: DFN-CERT-2012-0629
dfn-cert: DFN-CERT-2012-0610
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for libxml2 USN-1447-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1447-1

Vulnerability Detection Result

```
Vulnerable package: libxml2
Installed version:  2.6.31.dfsg-2ubuntu1
Fixed version:      2.6.31.dfsg-2ubuntu1.9
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

libxml2 on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Juri Aedla discovered that libxml2 contained an off by one error in its XPointer functionality. If a user or application linked against libxml2 were tricked into opening a specially crafted XML file, an attacker could cause the application to crash or possibly execute arbitrary code with the privileges of the user invoking the program.

Vulnerability Detection Method

Details: `Ubuntu Update for libxml2 USN-1447-1`
OID:1.3.6.1.4.1.25623.1.0.841007
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-3102
url: http://www.ubuntu.com/usn/usn-1447-1/
usn: 1447-1
cert-bund: CB-K14/0091
cert-bund: CB-K13/0874
cert-bund: CB-K13/0834
dfn-cert: DFN-CERT-2014-0093
dfn-cert: DFN-CERT-2013-0199
dfn-cert: DFN-CERT-2013-0196
dfn-cert: DFN-CERT-2012-1873
dfn-cert: DFN-CERT-2012-1841
dfn-cert: DFN-CERT-2012-1633
dfn-cert: DFN-CERT-2012-1218
dfn-cert: DFN-CERT-2012-1129
dfn-cert: DFN-CERT-2012-1027
dfn-cert: DFN-CERT-2012-0983
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for tiff USN-1631-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1631-1

Vulnerability Detection Result

```
Vulnerable package: libtiff4
Installed version:  3.8.2-7ubuntu3.4
Fixed version:      3.8.2-7ubuntu3.14
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

tiff on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that LibTIFF incorrectly handled certain malformed images using the PixarLog compression format. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. (CVE-2012-4447)
Huzaifa S. Sidhpurwala discovered that the ppm2tiff tool incorrectly handled certain malformed PPM images. If a user or automated system were tricked into opening a specially crafted PPM image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. (CVE-2012-4564)

Vulnerability Detection Method
Details: `Ubuntu Update for tiff USN-1631-1`
OID:1.3.6.1.4.1.25623.1.0.841216
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-4447
cve: CVE-2012-4564
url: http://www.ubuntu.com/usn/usn-1631-1/
usn: 1631-1
cert-bund: CB-K13/0930
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2013-1950
dfn-cert: DFN-CERT-2013-0944
dfn-cert: DFN-CERT-2013-0154
dfn-cert: DFN-CERT-2013-0006
dfn-cert: DFN-CERT-2012-2274
dfn-cert: DFN-CERT-2012-2136
dfn-cert: DFN-CERT-2012-2010
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for mysql-5.1 USN-1427-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1427-1

Vulnerability Detection Result

```
Vulnerable package: mysql-server-5.0
Installed version:  5.0.51a-3ubuntu5
Fixed version:      5.0.96-0ubuntu1
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
mysql-5.1 on Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.
MySQL has been updated to 5.1.62 in Ubuntu 10.04 LTS, Ubuntu 11.04 and Ubuntu 11.10. Ubuntu 8.04 LTS has been updated to MySQL 5.0.96.
In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.
Please see the references for more information.

Vulnerability Detection Method

Details: `Ubuntu Update for mysql-5.1 USN-1427-1`
OID:1.3.6.1.4.1.25623.1.0.840989
Version used: `2019-03-13T09:25:59Z`

References

```
url: http://www.ubuntu.com/usn/usn-1427-1/
usn: 1427-1
url: http://dev.mysql.com/doc/refman/5.1/en/news-5-1-62.html
url: http://dev.mysql.com/doc/refman/5.0/en/news-5-0-96.html
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for eglibc USN-1589-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1589-1

Vulnerability Detection Result

```
Vulnerable package: libc6
Installed version:  2.7-10ubuntu5
Fixed version:      2.7-10ubuntu8.2
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

eglibc on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

It was discovered that positional arguments to the printf() family of functions were not handled properly in the GNU C Library. An attacker could possibly use this to cause a stack-based buffer overflow, creating a denial of service or possibly execute arbitrary code. (CVE-2012-3404, CVE-2012-3405, CVE-2012-3406)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that multiple integer overflows existed in the strtod(), strtof() and strtold() functions in the GNU C Library. An attacker could possibly use this to trigger a stack-based buffer overflow, creating a denial of service or possibly execute arbitrary code. (CVE-2012-3480)

Vulnerability Detection Method

Details: `Ubuntu Update for eglibc USN-1589-1`
OID:1.3.6.1.4.1.25623.1.0.841171
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-3404
cve: CVE-2012-3405
cve: CVE-2012-3406
cve: CVE-2012-3480
url: http://www.ubuntu.com/usn/usn-1589-1/
usn: 1589-1
cert-bund: CB-K15/0473
cert-bund: CB-K15/0235
dfn-cert: DFN-CERT-2015-0484
dfn-cert: DFN-CERT-2015-0243
dfn-cert: DFN-CERT-2012-2288
dfn-cert: DFN-CERT-2012-1801
dfn-cert: DFN-CERT-2012-1669
dfn-cert: DFN-CERT-2012-1668
dfn-cert: DFN-CERT-2012-1614
dfn-cert: DFN-CERT-2012-1590
dfn-cert: DFN-CERT-2012-1403
dfn-cert: DFN-CERT-2012-1402
```

Medium (CVSS: 6.8)
NVT: Ubuntu Update for openssl USN-1451-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1451-1

Vulnerability Detection Result

```
Vulnerable package: libssl0.9.8
Installed version:  0.9.8g-4ubuntu3.18
Fixed version:      0.9.8g-4ubuntu3.19
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

openssl on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

Ivan Nestlerode discovered that the Cryptographic Message Syntax (CMS) and PKCS #7 implementations in OpenSSL returned early if RSA decryption failed. This could allow an attacker to expose sensitive information via a Million Message Attack (MMA). (CVE-2012-0884)
It was discovered that an integer underflow was possible when using TLS 1.1, TLS 1.2, or DTLS with CBC encryption. This could allow a remote attacker to cause a denial of service. (CVE-2012-2333)

Vulnerability Detection Method

Details: Ubuntu Update for openssl USN-1451-1
OID:1.3.6.1.4.1.25623.1.0.841013
Version used: 2019-03-13T09:25:59Z

References

cve: CVE-2012-0884
cve: CVE-2012-2333
url: http://www.ubuntu.com/usn/usn-1451-1/
usn: 1451-1
cert-bund: CB-K14/0854
dfn-cert: DFN-CERT-2014-0891
dfn-cert: DFN-CERT-2013-0512
dfn-cert: DFN-CERT-2013-0391
dfn-cert: DFN-CERT-2012-1581
dfn-cert: DFN-CERT-2012-1489
dfn-cert: DFN-CERT-2012-1382
dfn-cert: DFN-CERT-2012-1112
dfn-cert: DFN-CERT-2012-1075
dfn-cert: DFN-CERT-2012-1044
dfn-cert: DFN-CERT-2012-1038
dfn-cert: DFN-CERT-2012-1037
dfn-cert: DFN-CERT-2012-1036
dfn-cert: DFN-CERT-2012-1025
dfn-cert: DFN-CERT-2012-1013
dfn-cert: DFN-CERT-2012-0959
dfn-cert: DFN-CERT-2012-0957
dfn-cert: DFN-CERT-2012-0922
dfn-cert: DFN-CERT-2012-0888
dfn-cert: DFN-CERT-2012-0859
dfn-cert: DFN-CERT-2012-0761
dfn-cert: DFN-CERT-2012-0759
dfn-cert: DFN-CERT-2012-0669
dfn-cert: DFN-CERT-2012-0652
dfn-cert: DFN-CERT-2012-0558
dfn-cert: DFN-CERT-2012-0554

Medium (CVSS: 6.8)
NVT: Ubuntu Update for glibc USN-1589-2

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1589-2

Vulnerability Detection Result

```
Vulnerable package: libc6
Installed version:  2.7-10ubuntu5
Fixed version:      2.7-10ubuntu8.3
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
glibc on Ubuntu 8.04 LTS

Vulnerability Insight
USN-1589-1 fixed vulnerabilities in the GNU C Library. One of the updates exposed a regression in the floating point parser. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
It was discovered that positional arguments to the printf() family of functions were not handled properly in the GNU C Library. An attacker could possibly use this to cause a stack-based buffer overflow, creating a denial of service or possibly execute arbitrary code. (CVE-2012-3404, CVE-2012-3405, CVE-2012-3406) It was discovered that multiple integer overflows existed in the strtod(), strtof() and strtold() functions in the GNU C Library. An attacker could possibly use this to trigger a stack-based buffer overflow, creating a denial of service or possibly execute arbitrary code. (CVE-2012-3480)

Vulnerability Detection Method
Details: `Ubuntu Update for glibc USN-1589-2`
OID:1.3.6.1.4.1.25623.1.0.841254
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-3404
cve: CVE-2012-3405
cve: CVE-2012-3406
cve: CVE-2012-3480
url: http://www.ubuntu.com/usn/usn-1589-2/
usn: 1589-2
cert-bund: CB-K15/0473
cert-bund: CB-K15/0235
dfn-cert: DFN-CERT-2015-0484
dfn-cert: DFN-CERT-2015-0243
dfn-cert: DFN-CERT-2012-2288
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-1801
dfn-cert: DFN-CERT-2012-1669
dfn-cert: DFN-CERT-2012-1668
dfn-cert: DFN-CERT-2012-1614
dfn-cert: DFN-CERT-2012-1590
dfn-cert: DFN-CERT-2012-1403
dfn-cert: DFN-CERT-2012-1402
```

Medium (CVSS: 6.5)
NVT: Ubuntu Update for PostgreSQL vulnerability USN-1058-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1058-1

Vulnerability Detection Result

```
Vulnerable package: libpq5
Installed version:  8.3.1-1
Fixed version:      8.3.14-0ubuntu8.04
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
PostgreSQL vulnerability on Ubuntu 6.06 LTS, Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight
Geoff Keating reported that a buffer overflow exists in the intarray module's input function for the query_int type. This could allow an attacker to cause a denial of service or possibly execute arbitrary code as the postgres user.

Vulnerability Detection Method
Details: `Ubuntu Update for PostgreSQL vulnerability USN-1058-1`
OID:1.3.6.1.4.1.25623.1.0.840577
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2010-4015
url: http://www.ubuntu.com/usn/usn-1058-1/
usn: 1058-1
cert-bund: CB-K15/1514
dfn-cert: DFN-CERT-2012-1293
dfn-cert: DFN-CERT-2011-0492
dfn-cert: DFN-CERT-2011-0176
dfn-cert: DFN-CERT-2011-0151
dfn-cert: DFN-CERT-2011-0149
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-0146
dfn-cert: DFN-CERT-2011-0143
```

Medium (CVSS: 6.4)
NVT: Ubuntu Update for php5 USN-1307-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1307-1

Vulnerability Detection Result

```
Vulnerable package: php5-cgi
Installed version:  5.2.4-2ubuntu5.10
Fixed version:      5.2.4-2ubuntu5.19
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
php5 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Florent Hochwelker discovered that PHP incorrectly handled certain EXIF headers in JPEG files. A remote attacker could exploit this issue to view sensitive information or cause the PHP server to crash.

Vulnerability Detection Method
Details: `Ubuntu Update for php5 USN-1307-1`
OID:1.3.6.1.4.1.25623.1.0.840842
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-4566
url: http://www.ubuntu.com/usn/usn-1307-1/
usn: 1307-1
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0714
dfn-cert: DFN-CERT-2012-0586
dfn-cert: DFN-CERT-2012-0172
dfn-cert: DFN-CERT-2012-0167
dfn-cert: DFN-CERT-2012-0165
dfn-cert: DFN-CERT-2012-0130
dfn-cert: DFN-CERT-2012-0099
dfn-cert: DFN-CERT-2012-0070
dfn-cert: DFN-CERT-2012-0003
```

Medium (CVSS: 6.4)
NVT: Ubuntu Update for update-manager USN-1284-2

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1284-2

Vulnerability Detection Result

```
Vulnerable package: update-manager-core
Installed version:  0.87.24
Fixed version:      0.87.33
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
update-manager on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
USN-1284-1 fixed vulnerabilities in Update Manager. One of the fixes introduced a regression for Kubuntu users attempting to upgrade to a newer Ubuntu release. This update fixes the problem. We apologize for the inconvenience.
Original advisory details:
David Black discovered that Update Manager incorrectly extracted the downloaded upgrade tarball before verifying its GPG signature. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to replace arbitrary files. (CVE-2011-3152)
David Black discovered that Update Manager created a temporary directory in an insecure fashion. A local attacker could possibly use this flaw to read the XAUTHORITY file of the user performing the upgrade. (CVE-2011-3154)
This update also adds a hotfix to Update Notifier to handle cases where the upgrade is being performed from CD media.

Vulnerability Detection Method
Details: `Ubuntu Update for update-manager USN-1284-2`
OID:1.3.6.1.4.1.25623.1.0.840901
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-3152
cve: CVE-2011-3154
url: http://www.ubuntu.com/usn/usn-1284-2/
usn: 1284-2
```

Medium (CVSS: 5.8)
NVT: Ubuntu Update for gnupg USN-1682-1

Summary

... continues on next page ...

. . . continued from previous page . . .

The remote host is missing an update for the 'gnupg' package(s) announced via the referenced advisory.

Vulnerability Detection Result

```
Vulnerable package: gnupg
Installed version:  1.4.6-2ubuntu5
Fixed version:      1.4.6-2ubuntu5.2
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

gnupg on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

KB Sriram discovered that GnuPG incorrectly handled certain malformed keys. If a user or automated system were tricked into importing a malformed key, the GnuPG keyring could become corrupted.

Vulnerability Detection Method

Details: `Ubuntu Update for gnupg USN-1682-1`

OID:1.3.6.1.4.1.25623.1.0.841270

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-6085
url: http://www.ubuntu.com/usn/usn-1682-1/
usn: 1682-1
cert-bund: CB-K13/0837
cert-bund: CB-K13/0835
cert-bund: CB-K13/0776
dfn-cert: DFN-CERT-2013-1843
dfn-cert: DFN-CERT-2013-1841
dfn-cert: DFN-CERT-2013-1774
dfn-cert: DFN-CERT-2013-1084
dfn-cert: DFN-CERT-2013-1006
dfn-cert: DFN-CERT-2013-0090
dfn-cert: DFN-CERT-2013-0089
dfn-cert: DFN-CERT-2013-0065
dfn-cert: DFN-CERT-2013-0021
```

Medium (CVSS: 5.8)

NVT: Ubuntu Update for fuse vulnerability USN-1045-1

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Ubuntu Update for Linux kernel vulnerabilities USN-1045-1

Vulnerability Detection Result

```
Vulnerable package: fuse-utils
Installed version:  2.7.2-1ubuntu2
Fixed version:      2.7.2-1ubuntu2.2
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

fuse vulnerability on Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight

It was discovered that FUSE could be tricked into incorrectly updating the mtab file when mounting filesystems. A local attacker, with access to use FUSE, could unmount arbitrary locations, leading to a denial of service.

Vulnerability Detection Method

Details: `Ubuntu Update for fuse vulnerability USN-1045-1`
OID:1.3.6.1.4.1.25623.1.0.840568
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2010-3879
url: http://www.ubuntu.com/usn/usn-1045-1/
usn: 1045-1
dfn-cert: DFN-CERT-2011-1093
dfn-cert: DFN-CERT-2011-0492
dfn-cert: DFN-CERT-2011-0153
```

Medium (CVSS: 5.8)
NVT: Ubuntu Update for util-linux update USN-1045-2

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1045-2

Vulnerability Detection Result

```
Vulnerable package: bsdutils
Installed version:  2.13.1-5ubuntu1
Fixed version:      2.13.1-5ubuntu3.1
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

util-linux update on Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight

USN-1045-1 fixed vulnerabilities in FUSE. This update to util-linux adds support for new options required by the FUSE update.
Original advisory details:
It was discovered that FUSE could be tricked into incorrectly updating the mtab file when mounting filesystems. A local attacker, with access to use FUSE, could unmount arbitrary locations, leading to a denial of service.

Vulnerability Detection Method

Details: `Ubuntu Update for util-linux update USN-1045-2`
OID:1.3.6.1.4.1.25623.1.0.840569
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2010-3879
url: http://www.ubuntu.com/usn/usn-1045-2/
usn: 1045-2
dfn-cert: DFN-CERT-2011-1093
dfn-cert: DFN-CERT-2011-0492
dfn-cert: DFN-CERT-2011-0153
```

Medium (CVSS: 5.1)
NVT: Ubuntu Update for mysql-5.5 USN-1467-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1467-1

Vulnerability Detection Result

```
Vulnerable package: mysql-server-5.0
Installed version:  5.0.51a-3ubuntu5
Fixed version:      5.0.96-0ubuntu3
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

mysql-5.5 on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that certain builds of MySQL incorrectly handled password authentication on certain platforms. A remote attacker could use this issue to authenticate with an arbitrary password and establish a connection. (CVE-2012-2122)
MySQL has been updated to 5.5.24 in Ubuntu 12.04 LTS. Ubuntu 10.04 LTS, Ubuntu 11.04 and Ubuntu 11.10 have been updated to MySQL 5.1.63. A patch to fix the issue was backported to the version of MySQL in Ubuntu 8.04 LTS.
In addition to additional security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.
Please see the references for more information.

Vulnerability Detection Method
Details: `Ubuntu Update for mysql-5.5 USN-1467-1`
OID:1.3.6.1.4.1.25623.1.0.841039
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-2122
url: http://www.ubuntu.com/usn/usn-1467-1/
usn: 1467-1
url: http://dev.mysql.com/doc/refman/5.5/en/news-5-5-24.html
url: http://dev.mysql.com/doc/refman/5.1/en/news-5-1-63.html
dfn-cert: DFN-CERT-2013-0106
dfn-cert: DFN-CERT-2012-1563
dfn-cert: DFN-CERT-2012-1335
dfn-cert: DFN-CERT-2012-1256
dfn-cert: DFN-CERT-2012-1170
dfn-cert: DFN-CERT-2012-1163
```

Medium (CVSS: 5.0)
NVT: Ubuntu Update for apache2 USN-1259-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1259-1

Vulnerability Detection Result

```
Vulnerable package: apache2.2-common
Installed version:  2.2.8-1ubuntu0.15
Fixed version:      2.2.8-1ubuntu0.22
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
apache2 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that the mod_proxy module in Apache did not properly interact with the RewriteRule and ProxyPassMatch pattern matches in the configuration of a reverse proxy. This could allow remote attackers to contact internal webservers behind the proxy that were not intended for external exposure. (CVE-2011-3368)
Stefano Nichele discovered that the mod_proxy_ajp module in Apache when used with mod_proxy_balancer in certain configurations could allow remote attackers to cause a denial of service via a malformed HTTP request. (CVE-2011-3348)
Samuel Montosa discovered that the ITK Multi-Processing Module for Apache did not properly handle certain configuration sections that specify NiceValue but not AssignUserID, preventing Apache from dropping privileges correctly. This issue only affected Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-1176)
USN 1199-1 fixed a vulnerability in the byterange filter of Apache. The upstream patch introduced a regression in Apache when handling specific byte range requests. This update fixes the issue.
Original advisory details:
A flaw was discovered in the byterange filter in Apache. A remote attacker could exploit this to cause a denial of service via resource exhaustion.

Vulnerability Detection Method
Details: `Ubuntu Update for apache2 USN-1259-1`
OID:1.3.6.1.4.1.25623.1.0.840798
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-3368
cve: CVE-2011-3348
cve: CVE-2011-1176
url: http://www.ubuntu.com/usn/usn-1259-1/
usn: 1259-1
cert-bund: CB-K15/0080
cert-bund: CB-K14/1568
cert-bund: CB-K14/1505
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2014-1668
dfn-cert: DFN-CERT-2014-1592
dfn-cert: DFN-CERT-2013-1307
dfn-cert: DFN-CERT-2013-0237
dfn-cert: DFN-CERT-2012-0742
dfn-cert: DFN-CERT-2012-0741
dfn-cert: DFN-CERT-2012-0731
dfn-cert: DFN-CERT-2012-0568
dfn-cert: DFN-CERT-2012-0425
dfn-cert: DFN-CERT-2012-0343
dfn-cert: DFN-CERT-2012-0332
dfn-cert: DFN-CERT-2012-0228
dfn-cert: DFN-CERT-2012-0203
dfn-cert: DFN-CERT-2011-1726
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-1725
dfn-cert: DFN-CERT-2011-1693
dfn-cert: DFN-CERT-2011-1692
dfn-cert: DFN-CERT-2011-1632
dfn-cert: DFN-CERT-2011-1631
dfn-cert: DFN-CERT-2011-1567
dfn-cert: DFN-CERT-2011-1492
dfn-cert: DFN-CERT-2011-1430
dfn-cert: DFN-CERT-2011-0484
dfn-cert: DFN-CERT-2011-0435
```

Medium (CVSS: 5.0)
NVT: Ubuntu Update for apache2 USN-1765-1

Summary
The remote host is missing an update for the 'apache2' package(s) announced via the referenced advisory.

Vulnerability Detection Result

```
Vulnerable package: apache2.2-common
Installed version:  2.2.8-1ubuntu0.15
Fixed version:      2.2.8-1ubuntu0.25
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
apache2 on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Niels Heinen discovered that multiple modules incorrectly sanitized certain strings, which could result in browsers becoming vulnerable to cross-site scripting attacks when processing the output. With cross-site scripting vulnerabilities, if a user were tricked into viewing server output during a crafted server request, a remote attacker could exploit this to modify the contents, or steal confidential data (such as passwords), within the same domain. (CVE-2012-3499, CVE-2012-4558)
It was discovered that the mod_proxy_ajp module incorrectly handled error states. A remote attacker could use this issue to cause the server to stop responding, resulting in a denial of service. This issue only applied to Ubuntu 8.04 LTS, Ubuntu 10.04 LTS and Ubuntu 11.10. (CVE-2012-4557)
It was discovered that the apache2ctl script shipped in Ubuntu packages incorrectly created the lock directory. A local attacker could possibly use this issue to gain privileges. The symlink protections in Ubuntu 11.10 and later should reduce this vulnerability to a denial of service. (CVE-2013-1048)

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Details: `Ubuntu Update for apache2 USN-1765-1`
OID:1.3.6.1.4.1.25623.1.0.841365
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-3499
cve: CVE-2012-4558
cve: CVE-2012-4557
cve: CVE-2013-1048
url: http://www.ubuntu.com/usn/usn-1765-1/
usn: 1765-1
cert-bund: CB-K15/0960
cert-bund: CB-K14/0058
cert-bund: CB-K13/0600
dfn-cert: DFN-CERT-2015-1008
dfn-cert: DFN-CERT-2014-0049
dfn-cert: DFN-CERT-2013-1587
dfn-cert: DFN-CERT-2013-1307
dfn-cert: DFN-CERT-2013-1046
dfn-cert: DFN-CERT-2013-0944
dfn-cert: DFN-CERT-2013-0888
dfn-cert: DFN-CERT-2013-0716
dfn-cert: DFN-CERT-2013-0661
dfn-cert: DFN-CERT-2013-0476
dfn-cert: DFN-CERT-2013-0342
dfn-cert: DFN-CERT-2013-0237
dfn-cert: DFN-CERT-2012-2191
```

Medium (CVSS: 5.0)
NVT: Ubuntu Update for curl USN-1801-1

Summary

The remote host is missing an update for the 'curl' package(s) announced via the referenced advisory.

Vulnerability Detection Result

```
Vulnerable package: curl
Installed version:  7.18.0-1ubuntu2.3
Fixed version:      7.18.0-1ubuntu2.4
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

curl on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

YAMADA Yasuharu discovered that libcurl was vulnerable to a cookie leak when doing requests across domains with matching tails. curl did not properly restrict cookies to domains and subdomains. If a user or automated system were tricked into processing a specially crafted URL, an attacker could read cookie values stored by unrelated webservers.

Vulnerability Detection Method

Details: `Ubuntu Update for curl USN-1801-1`
OID:1.3.6.1.4.1.25623.1.0.841402
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2013-1944
usn: 1801-1
url: http://www.ubuntu.com/usn/usn-1801-1/
cert-bund: CB-K16/1107
cert-bund: CB-K14/1476
cert-bund: CB-K13/0845
cert-bund: CB-K13/0271
dfn-cert: DFN-CERT-2018-1365
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2014-1559
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1088
dfn-cert: DFN-CERT-2013-0977
dfn-cert: DFN-CERT-2013-0901
dfn-cert: DFN-CERT-2013-0867
dfn-cert: DFN-CERT-2013-0852
dfn-cert: DFN-CERT-2013-0835
dfn-cert: DFN-CERT-2013-0825
dfn-cert: DFN-CERT-2013-0808
```

Medium (CVSS: 5.0)
NVT: Ubuntu Update for samba vulnerability USN-1075-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1075-1

Vulnerability Detection Result

```
Vulnerable package: samba-common
Installed version:  3.0.20-0.1ubuntu1
Fixed version:      3.0.28a-1ubuntu4.14
```

Solution

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Please Install the Updated Packages.

Affected Software/OS

samba vulnerability on Ubuntu 6.06 LTS, Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight

Volker Lendecke discovered that Samba incorrectly handled certain file descriptors. A remote attacker could send a specially crafted request to the server and cause Samba to crash or hang, resulting in a denial of service.

Vulnerability Detection Method

Details: `Ubuntu Update for samba vulnerability USN-1075-1`
OID:1.3.6.1.4.1.25623.1.0.840597
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-0719
url: http://www.ubuntu.com/usn/usn-1075-1/
usn: 1075-1
dfn-cert: DFN-CERT-2012-1981
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0462
dfn-cert: DFN-CERT-2011-0962
dfn-cert: DFN-CERT-2011-0712
dfn-cert: DFN-CERT-2011-0399
dfn-cert: DFN-CERT-2011-0274
dfn-cert: DFN-CERT-2011-0268
dfn-cert: DFN-CERT-2011-0267
```

Medium (CVSS: 5.0)
NVT: Ubuntu Update for postgresql-8.4 USN-1229-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1229-1

Vulnerability Detection Result

```
Vulnerable package: postgresql-8.3
Installed version:  8.3.1-1
Fixed version:      8.3.16-0ubuntu0.8.04
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

. . . continues on next page . . .

... continued from previous page ...

postgresql-8.4 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

It was discovered that the blowfish algorithm in the pgcrypto module incorrectly handled certain 8-bit characters, resulting in the password hashes being easier to crack than expected. An attacker who could obtain the password hashes would be able to recover the plaintext with less effort.

Vulnerability Detection Method

Details: `Ubuntu Update for postgresql-8.4 USN-1229-1`
OID:1.3.6.1.4.1.25623.1.0.840772
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-2483
url: http://www.ubuntu.com/usn/usn-1229-1/
usn: 1229-1
cert-bund: CB-K15/1514
cert-bund: CB-K13/0921
dfn-cert: DFN-CERT-2013-1938
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0731
dfn-cert: DFN-CERT-2012-0678
dfn-cert: DFN-CERT-2012-0172
dfn-cert: DFN-CERT-2012-0167
dfn-cert: DFN-CERT-2011-1816
dfn-cert: DFN-CERT-2011-1814
dfn-cert: DFN-CERT-2011-1813
dfn-cert: DFN-CERT-2011-1708
dfn-cert: DFN-CERT-2011-1698
dfn-cert: DFN-CERT-2011-1686
dfn-cert: DFN-CERT-2011-1643
dfn-cert: DFN-CERT-2011-1603
dfn-cert: DFN-CERT-2011-1602
dfn-cert: DFN-CERT-2011-1443
dfn-cert: DFN-CERT-2011-1433
dfn-cert: DFN-CERT-2011-1402
dfn-cert: DFN-CERT-2011-1396
dfn-cert: DFN-CERT-2011-1387
dfn-cert: DFN-CERT-2011-1276
```

Medium (CVSS: 5.0)
NVT: Ubuntu Update for expat USN-1527-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1527-1

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable package: libexpat1
Installed version:  2.0.1-0ubuntu1
Fixed version:      2.0.1-0ubuntu1.2
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

expat on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

It was discovered that Expat computed hash values without restricting the ability to trigger hash collisions predictably. If a user or application linked against Expat were tricked into opening a crafted XML file, an attacker could cause a denial of service by consuming excessive CPU resources. (CVE-2012-0876)

Tim Boddy discovered that Expat did not properly handle memory reallocation when processing XML files. If a user or application linked against Expat were tricked into opening a crafted XML file, an attacker could cause a denial of service by consuming excessive memory resources. This issue only affected Ubuntu 8.04 LTS, 10.04 LTS, 11.04 and 11.10. (CVE-2012-1148)

Vulnerability Detection Method

Details: `Ubuntu Update for expat USN-1527-1`

OID:1.3.6.1.4.1.25623.1.0.841101

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-0876
cve: CVE-2012-1148
url: http://www.ubuntu.com/usn/usn-1527-1/
usn: 1527-1
cert-bund: CB-K17/0536
cert-bund: CB-K17/0492
cert-bund: CB-K16/1972
cert-bund: CB-K16/1816
cert-bund: CB-K16/0112
cert-bund: CB-K15/1792
cert-bund: CB-K15/0987
cert-bund: CB-K13/0845
dfn-cert: DFN-CERT-2020-0405
dfn-cert: DFN-CERT-2017-0551
dfn-cert: DFN-CERT-2017-0508
dfn-cert: DFN-CERT-2016-2081
dfn-cert: DFN-CERT-2016-1923
dfn-cert: DFN-CERT-2016-0125
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-1898
dfn-cert: DFN-CERT-2015-1035
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2012-2129
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1522
dfn-cert: DFN-CERT-2012-1513
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1133
dfn-cert: DFN-CERT-2012-0948
dfn-cert: DFN-CERT-2012-0835
dfn-cert: DFN-CERT-2012-0693
dfn-cert: DFN-CERT-2012-0567
dfn-cert: DFN-CERT-2012-0559
```

Medium (CVSS: 5.0)
NVT: Ubuntu Update for php5 regression USN-1042-2

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1042-2

Vulnerability Detection Result

```
Vulnerable package: php5-cgi
Installed version:  5.2.4-2ubuntu5.10
Fixed version:      5.2.4-2ubuntu5.14
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
php5 regression on Ubuntu 6.06 LTS, Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight
USN-1042-1 fixed vulnerabilities in PHP5. The fix for CVE-2010-3436 introduced a regression in the open_basedir restriction handling code. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
It was discovered that attackers might be able to bypass open_basedir() restrictions by passing a specially crafted filename. (CVE-2010-3436)

Vulnerability Detection Method
Details: `Ubuntu Update for php5 regression USN-1042-2`
OID:1.3.6.1.4.1.25623.1.0.840566

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2010-3436
url: http://www.ubuntu.com/usn/usn-1042-2/
usn: 1042-2
dfn-cert: DFN-CERT-2012-0731
dfn-cert: DFN-CERT-2011-0013
dfn-cert: DFN-CERT-2011-0012
dfn-cert: DFN-CERT-2011-0011
dfn-cert: DFN-CERT-2010-1471
```

Medium (CVSS: 5.0)
NVT: Ubuntu Update for openssl USN-1732-1

Summary

The remote host is missing an update for the 'openssl' package(s) announced via the referenced advisory.

Vulnerability Detection Result

```
Vulnerable package: libssl0.9.8
Installed version:  0.9.8g-4ubuntu3.18
Fixed version:      0.9.8g-4ubuntu3.20
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

openssl on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

Adam Langley and Wolfgang Ettlingers discovered that OpenSSL incorrectly handled certain crafted CBC data when used with AES-NI. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service. This issue only affected Ubuntu 12.04 LTS and Ubuntu 12.10. (CVE-2012-2686)
Stephen Henson discovered that OpenSSL incorrectly performed signature verification for OCSP responses. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service. (CVE-2013-0166)
Nadhem Alfardan and Kenny Paterson discovered that the TLS protocol as used in OpenSSL was vulnerable to a timing side-channel attack known as the 'Lucky Thirteen' issue. A remote attacker could use this issue to perform plaintext-recovery attacks via analysis of timing data. (CVE-2013-0169)

Vulnerability Detection Method

Details: `Ubuntu Update for openssl USN-1732-1`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.841327
Version used: 2019-03-13T09:25:59Z

References

```
cve: CVE-2012-2686
cve: CVE-2013-0166
cve: CVE-2013-0169
url: http://www.ubuntu.com/usn/usn-1732-1/
usn: 1732-1
cert-bund: CB-K20/1049
cert-bund: CB-K15/0384
cert-bund: CB-K14/1537
cert-bund: CB-K14/1241
cert-bund: CB-K14/0458
cert-bund: CB-K14/0262
cert-bund: CB-K13/0823
cert-bund: CB-K13/0801
cert-bund: CB-K13/0796
cert-bund: CB-K13/0794
cert-bund: CB-K13/0790
cert-bund: CB-K13/0462
cert-bund: CB-K13/0096
cert-bund: CB-K13/0093
dfn-cert: DFN-CERT-2020-2335
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1306
dfn-cert: DFN-CERT-2014-0483
dfn-cert: DFN-CERT-2014-0262
dfn-cert: DFN-CERT-2013-1821
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2013-1391
dfn-cert: DFN-CERT-2013-1307
dfn-cert: DFN-CERT-2013-1046
dfn-cert: DFN-CERT-2013-0990
dfn-cert: DFN-CERT-2013-0945
dfn-cert: DFN-CERT-2013-0911
dfn-cert: DFN-CERT-2013-0910
dfn-cert: DFN-CERT-2013-0830
dfn-cert: DFN-CERT-2013-0805
dfn-cert: DFN-CERT-2013-0722
dfn-cert: DFN-CERT-2013-0672
dfn-cert: DFN-CERT-2013-0670
dfn-cert: DFN-CERT-2013-0512
dfn-cert: DFN-CERT-2013-0470
dfn-cert: DFN-CERT-2013-0469
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2013-0467
dfn-cert: DFN-CERT-2013-0461
dfn-cert: DFN-CERT-2013-0457
dfn-cert: DFN-CERT-2013-0401
dfn-cert: DFN-CERT-2013-0395
dfn-cert: DFN-CERT-2013-0393
dfn-cert: DFN-CERT-2013-0391
dfn-cert: DFN-CERT-2013-0379
dfn-cert: DFN-CERT-2013-0378
dfn-cert: DFN-CERT-2013-0362
dfn-cert: DFN-CERT-2013-0352
dfn-cert: DFN-CERT-2013-0304
dfn-cert: DFN-CERT-2013-0301
```

Medium (CVSS: 5.0)
NVT: Ubuntu Update for gnutls26 USN-1418-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1418-1

Vulnerability Detection Result

```
Vulnerable package: libgnutls13
Installed version:  2.0.4-1ubuntu2
Fixed version:      2.0.4-1ubuntu2.7
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
gnutls26 on Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Alban Crequy discovered that the GnuTLS library incorrectly checked array bounds when copying TLS session data. A remote attacker could crash a client application, leading to a denial of service, as the client application prepared for TLS session resumption. (CVE-2011-4128)
Matthew Hall discovered that the GnuTLS library incorrectly handled TLS records. A remote attacker could crash client and server applications, leading to a denial of service, by sending a crafted TLS record. (CVE-2012-1573)

Vulnerability Detection Method
Details: `Ubuntu Update for gnutls26 USN-1418-1`
OID:1.3.6.1.4.1.25623.1.0.840978
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-4128
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2012-1573
url: http://www.ubuntu.com/usn/usn-1418-1/
usn: 1418-1
cert-bund: CB-K14/0262
dfn-cert: DFN-CERT-2014-0262
dfn-cert: DFN-CERT-2012-1988
dfn-cert: DFN-CERT-2012-1987
dfn-cert: DFN-CERT-2012-1697
dfn-cert: DFN-CERT-2012-0943
dfn-cert: DFN-CERT-2012-0651
dfn-cert: DFN-CERT-2012-0601
dfn-cert: DFN-CERT-2012-0561
dfn-cert: DFN-CERT-2012-0560
dfn-cert: DFN-CERT-2012-0556
dfn-cert: DFN-CERT-2012-0542
dfn-cert: DFN-CERT-2012-0541
dfn-cert: DFN-CERT-2012-0244
```

Medium (CVSS: 5.0)
NVT: Pidgin MSN Protocol Plugin Denial Of Service Vulnerability (Linux)

Product detection result

```
cpe:/a:pidgin:pidgin:2.5.2
Detected by Pidgin Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.900661)
```

Summary
This host has Pidgin installed and is prone to Denial Of Service vulnerability

Vulnerability Detection Result

```
Installed version: 2.5.2
Fixed version:     2.6.6
```

Impact
Attackers can exploit this issue to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.

Solution
Solution type: VendorFix
Upgrade to Pidgin version 2.6.6 or later.

Affected Software/OS
Pidgin version prior to 2.6.6 on Linux.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

This issue is due to an error in 'slp.c' within the 'MSN protocol plugin' in 'libpurple' when processing MSN request.

Vulnerability Detection Method
Details: `Pidgin MSN Protocol Plugin Denial Of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800424
Version used: `2018-12-05T14:14:20Z`

Product Detection Result
Product: `cpe:/a:pidgin:pidgin:2.5.2`
Method: `Pidgin Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.900661)

References

```
cve: CVE-2010-0277
url: http://www.openwall.com/lists/oss-security/2010/01/07/2
dfn-cert: DFN-CERT-2010-1647
dfn-cert: DFN-CERT-2010-1533
dfn-cert: DFN-CERT-2010-0605
dfn-cert: DFN-CERT-2010-0348
dfn-cert: DFN-CERT-2010-0258
dfn-cert: DFN-CERT-2010-0246
dfn-cert: DFN-CERT-2010-0242
```

Medium (CVSS: 5.0)
NVT: Ubuntu Update for gnupg USN-1570-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1570-1

Vulnerability Detection Result

```
Vulnerable package: gnupg
Installed version:  1.4.6-2ubuntu5
Fixed version:      1.4.6-2ubuntu5.1
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
gnupg on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that GnuPG used a short ID when downloading keys from a keyserver, even if a long ID was requested. An attacker could possibly use this to return a different key with a duplicate short key id.

Vulnerability Detection Method
Details: `Ubuntu Update for gnupg USN-1570-1`
OID:1.3.6.1.4.1.25623.1.0.841152
Version used: `2019-03-13T09:25:59Z`

References
```
url: http://www.ubuntu.com/usn/usn-1570-1/
usn: 1570-1
```

Medium (CVSS: 5.0)
NVT: Ubuntu Update for libxml2 USN-1376-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1376-1

Vulnerability Detection Result
```
Vulnerable package: libxml2
Installed version:  2.6.31.dfsg-2ubuntu1
Fixed version:      2.6.31.dfsg-2ubuntu1.8
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
libxml2 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Juraj Somorovsky discovered that libxml2 was vulnerable to hash table collisions. If a user or application linked against libxml2 were tricked into opening a specially crafted XML file, an attacker could cause a denial of service.

Vulnerability Detection Method
Details: `Ubuntu Update for libxml2 USN-1376-1`
OID:1.3.6.1.4.1.25623.1.0.840917
Version used: `2019-03-13T09:25:59Z`

References
```
cve: CVE-2012-0841
url: http://www.ubuntu.com/usn/usn-1376-1/
usn: 1376-1
cert-bund: CB-K15/0050
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K14/0091
cert-bund: CB-K13/0874
dfn-cert: DFN-CERT-2015-0049
dfn-cert: DFN-CERT-2014-0093
dfn-cert: DFN-CERT-2013-0196
dfn-cert: DFN-CERT-2012-1873
dfn-cert: DFN-CERT-2012-1697
dfn-cert: DFN-CERT-2012-1634
dfn-cert: DFN-CERT-2012-1361
dfn-cert: DFN-CERT-2012-0562
dfn-cert: DFN-CERT-2012-0452
dfn-cert: DFN-CERT-2012-0352
dfn-cert: DFN-CERT-2012-0347
dfn-cert: DFN-CERT-2012-0345
```

Medium (CVSS: 5.0)
NVT: Pidgin OSCAR Protocol Denial Of Service Vulnerability (Linux)

Product detection result

```
cpe:/a:pidgin:pidgin:2.5.2
Detected by Pidgin Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.900661)
```

Summary

This host has installed Pidgin and is prone to Denial of Service vulnerability.

Vulnerability Detection Result

```
Installed version: 2.5.2
Fixed version:     2.5.8
```

Impact

Successful exploitation will allow attacker to cause an application crash.

Solution

Solution type: VendorFix

Upgrade to Pidgin version 2.5.8.

Affected Software/OS

Pidgin version prior to 2.5.8 on Linux

Vulnerability Insight

Error in OSCAR protocol implementation leads to the application misinterpreting the ICQWebMessage message type as ICQSMS message type via a crafted ICQ web message that triggers allocation of a large amount of memory.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Pidgin OSCAR Protocol Denial Of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800824
Version used: `2020-11-12T09:50:32Z`

Product Detection Result
Product: `cpe:/a:pidgin:pidgin:2.5.2`
Method: `Pidgin Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.900661)

References

```
cve: CVE-2009-1889
bid: 35530
url: http://secunia.com/advisories/35652
url: http://developer.pidgin.im/ticket/9483
url: http://pidgin.im/pipermail/devel/2009-May/008227.html
dfn-cert: DFN-CERT-2009-1707
dfn-cert: DFN-CERT-2009-1116
```

Medium (CVSS: 5.0)
NVT: Pidgin Multiple Denial Of Service Vulnerabilities (Linux)

Product detection result

```
cpe:/a:pidgin:pidgin:2.5.2
Detected by Pidgin Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.900661)
```

Summary
This host has Pidgin installed and is prone to multiple Denial of Service vulnerabilities.

Vulnerability Detection Result

```
Installed version: 2.5.2
Fixed version:     2.6.2
```

Impact
Attackers can exploit this issue to execute arbitrary code, corrupt memory and cause the application to crash.

Solution
Solution type: VendorFix
Upgrade to Pidgin version 2.6.2.

Affected Software/OS
Pidgin version prior to 2.6.2 on Linux.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

- An error in libpurple/protocols/irc/msgs.c in the IRC protocol plugin in libpurple can trigger a NULL-pointer dereference when processing TOPIC messages which lack a topic string.
- An error in the 'msn_slp_sip_recv' function in libpurple/protocols/msn/slp.c in the MSN protocol can trigger a NULL-pointer dereference via an SLP invite message missing expected fields.
- An error in the 'msn_slp_process_msg' function in libpurple/protocols/msn/ slpcall.c in the MSN protocol when converting the encoding of a handwritten message can be exploited by improper utilisation of uninitialised variables.
- An error in the XMPP protocol plugin in libpurple is fails to handle an error IQ stanza during an attempted fetch of a custom smiley is processed via XHTML-IM content with cid: images.

Vulnerability Detection Method
Details: `Pidgin Multiple Denial Of Service Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900941
Version used: `2018-12-05T14:14:20Z`

Product Detection Result
Product: `cpe:/a:pidgin:pidgin:2.5.2`
Method: `Pidgin Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.900661)

References
```
cve: CVE-2009-2703
cve: CVE-2009-3083
cve: CVE-2009-3084
cve: CVE-2009-3085
bid: 36277
url: http://secunia.com/advisories/36601
url: http://developer.pidgin.im/ticket/10159
url: http://www.pidgin.im/news/security/?id=37
url: http://www.pidgin.im/news/security/?id=38
url: http://www.pidgin.im/news/security/?id=39
url: http://www.pidgin.im/news/security/?id=40
dfn-cert: DFN-CERT-2010-0036
dfn-cert: DFN-CERT-2009-1707
dfn-cert: DFN-CERT-2009-1537
dfn-cert: DFN-CERT-2009-1321
dfn-cert: DFN-CERT-2009-1283
```

Medium (CVSS: 5.0)
NVT: Ubuntu Update for libgc USN-1546-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1546-1

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable package: libgc1c2
Installed version:  6.8-1.1
Fixed version:      1:6.8-1.1ubuntu0.1
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
libgc on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that multiple integer overflows existed in the malloc and calloc implementations in the Boehm-Demers-Weiser garbage collecting memory allocator (libgc). These could allow an attacker to cause a denial of service or possibly execute arbitrary code.

Vulnerability Detection Method
Details: `Ubuntu Update for libgc USN-1546-1`
OID:1.3.6.1.4.1.25623.1.0.841125
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-2673
url: http://www.ubuntu.com/usn/usn-1546-1/
usn: 1546-1
cert-bund: CB-K13/0875
dfn-cert: DFN-CERT-2013-1888
dfn-cert: DFN-CERT-2012-1265
```

Medium (CVSS: 5.0)
NVT: Ubuntu Update for libtasn1-3 USN-1436-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1436-1

Vulnerability Detection Result

```
Vulnerable package: libtasn1-3
Installed version:  1.1-1
Fixed version:      1.1-1ubuntu0.1
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

libtasn1-3 on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

Matthew Hall discovered that Libtasn1 incorrectly handled certain large values. An attacker could exploit this with a specially crafted ASN.1 structure and cause a denial of service, or possibly execute arbitrary code.

Vulnerability Detection Method

Details: `Ubuntu Update for libtasn1-3 USN-1436-1`
OID:1.3.6.1.4.1.25623.1.0.840994
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-1569
url: http://www.ubuntu.com/usn/usn-1436-1/
usn: 1436-1
cert-bund: CB-K14/0262
dfn-cert: DFN-CERT-2014-0262
dfn-cert: DFN-CERT-2012-1697
dfn-cert: DFN-CERT-2012-0943
dfn-cert: DFN-CERT-2012-0707
dfn-cert: DFN-CERT-2012-0691
dfn-cert: DFN-CERT-2012-0667
dfn-cert: DFN-CERT-2012-0635
dfn-cert: DFN-CERT-2012-0606
dfn-cert: DFN-CERT-2012-0605
dfn-cert: DFN-CERT-2012-0561
dfn-cert: DFN-CERT-2012-0557
dfn-cert: DFN-CERT-2012-0549
dfn-cert: DFN-CERT-2012-0544
```

Medium (CVSS: 5.0)
NVT: Pidgin Oscar Protocol Denial of Service Vulnerability (Linux)

Product detection result

```
cpe:/a:pidgin:pidgin:2.5.2
Detected by Pidgin Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.900661)
```

Summary

This host has Pidgin installed and is prone to Denial of Service vulnerability.

Vulnerability Detection Result

```
Installed version: 2.5.2
Fixed version:     2.6.3
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow attacker to cause a Denial of Service.

Solution

Solution type: VendorFix

Upgrade to Pidgin version 2.6.3.

Affected Software/OS

Pidgin version prior to 2.6.3 on Linux.

Vulnerability Insight

This issue is caused by an error in the Oscar protocol plugin when processing malformed ICQ or AIM contacts sent by the SIM IM client, which could cause an invalid memory access leading to a crash.

Vulnerability Detection Method

Details: `Pidgin Oscar Protocol Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.801031
Version used: `2018-12-05T14:14:20Z`

Product Detection Result

Product: `cpe:/a:pidgin:pidgin:2.5.2`
Method: `Pidgin Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.900661)

References

```
cve: CVE-2009-3615
bid: 36719
url: http://secunia.com/advisories/37072
url: http://xforce.iss.net/xforce/xfdb/53807
url: http://www.pidgin.im/news/security/?id=41
url: http://developer.pidgin.im/wiki/ChangeLog
dfn-cert: DFN-CERT-2010-0605
dfn-cert: DFN-CERT-2010-0036
dfn-cert: DFN-CERT-2010-0035
dfn-cert: DFN-CERT-2009-1604
dfn-cert: DFN-CERT-2009-1575
dfn-cert: DFN-CERT-2009-1537
dfn-cert: DFN-CERT-2009-1489
```

Medium (CVSS: 4.9)
NVT: Ubuntu Update for postgresql-9.1 USN-1542-1

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Ubuntu Update for Linux kernel vulnerabilities USN-1542-1

Vulnerability Detection Result

```
Vulnerable package: postgresql-8.3
Installed version:  8.3.1-1
Fixed version:      8.3.20-0ubuntu8.04
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

postgresql-9.1 on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

Peter Eisentraut discovered that the XSLT functionality in the optional XML2 extension would allow unprivileged database users to both read and write data with the privileges of the database server. (CVE-2012-3488)
Noah Misch and Tom Lane discovered that the XML functionality in the optional XML2 extension would allow unprivileged database users to read data with the privileges of the database server. (CVE-2012-3489)

Vulnerability Detection Method

Details: `Ubuntu Update for postgresql-9.1 USN-1542-1`
OID:1.3.6.1.4.1.25623.1.0.841120
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-3488
cve: CVE-2012-3489
url: http://www.ubuntu.com/usn/usn-1542-1/
usn: 1542-1
cert-bund: CB-K15/1514
dfn-cert: DFN-CERT-2012-1940
dfn-cert: DFN-CERT-2012-1922
dfn-cert: DFN-CERT-2012-1917
dfn-cert: DFN-CERT-2012-1878
dfn-cert: DFN-CERT-2012-1776
dfn-cert: DFN-CERT-2012-1770
dfn-cert: DFN-CERT-2012-1659
dfn-cert: DFN-CERT-2012-1658
dfn-cert: DFN-CERT-2012-1611
```

Medium (CVSS: 4.6)
NVT: Ubuntu Update for bzip2 USN-1308-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1308-1

Vulnerability Detection Result

```
Vulnerable package: bzip2
Installed version:  1.0.4-2ubuntu4
Fixed version:      1.0.4-2ubuntu4.2
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
bzip2 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
vladz discovered that executables compressed by bzexe insecurely create temporary files when they are ran. A local attacker could exploit this issue to execute arbitrary code as the user running a compressed executable.

Vulnerability Detection Method
Details: `Ubuntu Update for bzip2 USN-1308-1`
OID:1.3.6.1.4.1.25623.1.0.840839
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-4089
url: http://www.ubuntu.com/usn/usn-1308-1/
usn: 1308-1
```

Medium (CVSS: 4.6)
NVT: Ubuntu Update for apache2 USN-1368-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1368-1

Vulnerability Detection Result

```
Vulnerable package: apache2.2-common
Installed version:  2.2.8-1ubuntu0.15
Fixed version:      2.2.8-1ubuntu0.23
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
apache2 on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that the Apache HTTP Server incorrectly handled the SetEnvIf .htaccess file directive. An attacker having write access to a .htaccess file may exploit this to possibly execute arbitrary code. (CVE-2011-3607)
Prutha Parikh discovered that the mod_proxy module did not properly interact with the RewriteRule and ProxyPassMatch pattern matches in the configuration of a reverse proxy. This could allow remote attackers to contact internal webservers behind the proxy that were not intended for external exposure. (CVE-2011-4317)
Rainer Canavan discovered that the mod_log_config module incorrectly handled a certain format string when used with a threaded MPM. A remote attacker could exploit this to cause a denial of service via a specially- crafted cookie. This issue only affected Ubuntu 11.04 and 11.10. (CVE-2012-0021)
It was discovered that the Apache HTTP Server incorrectly handled certain type fields within a scoreboard shared memory segment. A local attacker could exploit this to cause a denial of service. (CVE-2012-0031)
Norman Hippert discovered that the Apache HTTP Server incorrectly handled header information when returning a Bad Request (400) error page. A remote attacker could exploit this to obtain the values of certain HTTPOnly cookies. (CVE-2012-0053)

Vulnerability Detection Method
Details: `Ubuntu Update for apache2 USN-1368-1`
OID:1.3.6.1.4.1.25623.1.0.840900
Version used: `2020-06-09T14:44:58Z`

References
```
cve: CVE-2011-3607
cve: CVE-2011-4317
cve: CVE-2012-0021
cve: CVE-2012-0031
cve: CVE-2012-0053
url: http://www.ubuntu.com/usn/usn-1368-1/
usn: 1368-1
cert-bund: CB-K15/1073
cert-bund: CB-K15/0080
cert-bund: CB-K15/0079
cert-bund: CB-K14/1505
cert-bund: CB-K14/0608
dfn-cert: DFN-CERT-2015-1135
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2014-1592
dfn-cert: DFN-CERT-2014-0635
dfn-cert: DFN-CERT-2013-1307
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2013-0237
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1112
dfn-cert: DFN-CERT-2012-0928
dfn-cert: DFN-CERT-2012-0771
dfn-cert: DFN-CERT-2012-0758
dfn-cert: DFN-CERT-2012-0744
dfn-cert: DFN-CERT-2012-0743
dfn-cert: DFN-CERT-2012-0740
dfn-cert: DFN-CERT-2012-0731
dfn-cert: DFN-CERT-2012-0568
dfn-cert: DFN-CERT-2012-0425
dfn-cert: DFN-CERT-2012-0424
dfn-cert: DFN-CERT-2012-0387
dfn-cert: DFN-CERT-2012-0343
dfn-cert: DFN-CERT-2012-0332
dfn-cert: DFN-CERT-2012-0306
dfn-cert: DFN-CERT-2012-0264
dfn-cert: DFN-CERT-2012-0228
dfn-cert: DFN-CERT-2012-0203
dfn-cert: DFN-CERT-2012-0188
dfn-cert: DFN-CERT-2012-0048
```

Medium (CVSS: 4.4)
NVT: Insecure Saving Of Downloadable File In Mozilla Firefox (Linux)

Summary
This host is installed with Mozilla Firefox and is prone to insecure saving of downloadable file.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Local attackers may leverage this issue by replacing an arbitrary downloaded file by placing a file in a /tmp location before the download occurs.

Solution
Solution type: VendorFix
Upgrade to Mozilla Firefox version 3.6.3 or later

Affected Software/OS
Mozilla Firefox version 2.x, 3.x on Linux.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

This security issue is due to the browser using a fixed path from the /tmp directory when a user opens a file downloaded for opening from the 'Downloads' window. This can be exploited to trick a user into opening a file with potentially malicious content by placing it in the /tmp directory before the download takes place.

Vulnerability Detection Method

Details: `Insecure Saving Of Downloadable File In Mozilla Firefox (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900869
Version used: `2020-10-20T15:03:35Z`

References

```
cve: CVE-2009-3274
url: http://secunia.com/advisories/36649
url: http://jbrownsec.blogspot.com/2009/09/vamos-updates.html
url: http://securitytube.net/Zero-Day-Demos-%28Firefox-Vulnerability-Discovered%
↪29-video.aspx
dfn-cert: DFN-CERT-2010-0593
dfn-cert: DFN-CERT-2010-0369
dfn-cert: DFN-CERT-2010-0014
dfn-cert: DFN-CERT-2009-1661
dfn-cert: DFN-CERT-2009-1564
dfn-cert: DFN-CERT-2009-1563
dfn-cert: DFN-CERT-2009-1554
dfn-cert: DFN-CERT-2009-1535
dfn-cert: DFN-CERT-2009-1532
dfn-cert: DFN-CERT-2009-1531
dfn-cert: DFN-CERT-2009-1525
dfn-cert: DFN-CERT-2009-1524
```

Medium (CVSS: 4.3)
NVT: Ubuntu Update for freetype USN-1686-1

Summary

The remote host is missing an update for the 'freetype' package(s) announced via the referenced advisory.

Vulnerability Detection Result

```
Vulnerable package: libfreetype6
Installed version:  2.3.5-1ubuntu4.8.04.2
Fixed version:      2.3.5-1ubuntu4.8.04.10
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

freetype on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed BDF font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges.

Vulnerability Detection Method

Details: `Ubuntu Update for freetype USN-1686-1`
OID:1.3.6.1.4.1.25623.1.0.841275
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-5668
cve: CVE-2012-5669
cve: CVE-2012-5670
url: http://www.ubuntu.com/usn/usn-1686-1/
usn: 1686-1
cert-bund: CB-K16/0173
dfn-cert: DFN-CERT-2016-0188
dfn-cert: DFN-CERT-2013-0266
dfn-cert: DFN-CERT-2013-0225
dfn-cert: DFN-CERT-2013-0193
dfn-cert: DFN-CERT-2013-0157
dfn-cert: DFN-CERT-2013-0128
dfn-cert: DFN-CERT-2013-0127
```

Medium (CVSS: 4.3)
NVT: Ubuntu Update for libxml2 USN-1782-1

Summary

The remote host is missing an update for the 'libxml2' package(s) announced via the referenced advisory.

Vulnerability Detection Result

```
Vulnerable package: libxml2
Installed version:  2.6.31.dfsg-2ubuntu1
Fixed version:      2.6.31.dfsg-2ubuntu1.12
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

libxml2 on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

It was discovered that libxml2 incorrectly handled XML entity expansion. An attacker could use this flaw to cause libxml2 to consume large amounts of resources, resulting in a denial of service.

Vulnerability Detection Method

Details: `Ubuntu Update for libxml2 USN-1782-1`
OID:1.3.6.1.4.1.25623.1.0.841380
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2013-0338
url: http://www.ubuntu.com/usn/usn-1782-1/
usn: 1782-1
cert-bund: CB-K15/0079
cert-bund: CB-K15/0050
cert-bund: CB-K13/0874
cert-bund: CB-K13/0823
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0049
dfn-cert: DFN-CERT-2013-1821
dfn-cert: DFN-CERT-2013-1391
dfn-cert: DFN-CERT-2013-1307
dfn-cert: DFN-CERT-2013-1046
dfn-cert: DFN-CERT-2013-0944
dfn-cert: DFN-CERT-2013-0651
dfn-cert: DFN-CERT-2013-0649
dfn-cert: DFN-CERT-2013-0435
```

Medium (CVSS: 4.3)
NVT: Ubuntu Update for apr USN-1134-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1134-1

Vulnerability Detection Result

```
Vulnerable package: libapr1
Installed version:  1.2.11-1
Fixed version:      1.2.11-1ubuntu0.2
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

apr on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS, Ubuntu 6.06 LTS

Vulnerability Insight

Maksymilian Arciemowicz reported that a flaw in the fnmatch() implementation in the Apache Portable Runtime (APR) library could allow an attacker to cause a denial of service. This can be demonstrated in a remote denial of service attack against mod_autoindex in the Apache web server. (CVE-2011-0419)

Is was discovered that the fix for CVE-2011-0419 introduced a different flaw in the fnmatch() implementation that could also result in a denial of service. (CVE-2011-1928)

Vulnerability Detection Method

Details: `Ubuntu Update for apr USN-1134-1`

OID:1.3.6.1.4.1.25623.1.0.840667

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-0419
cve: CVE-2011-1928
url: http://www.ubuntu.com/usn/usn-1134-1/
usn: 1134-1
cert-bund: CB-K14/1599
dfn-cert: DFN-CERT-2014-1694
dfn-cert: DFN-CERT-2013-1307
dfn-cert: DFN-CERT-2013-0784
dfn-cert: DFN-CERT-2012-1406
dfn-cert: DFN-CERT-2012-0731
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0150
dfn-cert: DFN-CERT-2011-1725
dfn-cert: DFN-CERT-2011-1692
dfn-cert: DFN-CERT-2011-1492
dfn-cert: DFN-CERT-2011-1379
dfn-cert: DFN-CERT-2011-0876
dfn-cert: DFN-CERT-2011-0863
dfn-cert: DFN-CERT-2011-0848
dfn-cert: DFN-CERT-2011-0802
dfn-cert: DFN-CERT-2011-0762
dfn-cert: DFN-CERT-2011-0761
dfn-cert: DFN-CERT-2011-0748
```

Medium (CVSS: 4.3)
NVT: Ubuntu Update for postgresql-9.1 USN-1461-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1461-1

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable package: postgresql-8.3
Installed version:  8.3.1-1
Fixed version:      8.3.19-0ubuntu8.04
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

postgresql-9.1 on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

It was discovered that PostgreSQL incorrectly handled certain bytes passed to the crypt() function when using DES encryption. An attacker could use this flaw to incorrectly handle authentication. (CVE-2012-2143)

It was discovered that PostgreSQL incorrectly handled SECURITY DEFINER and SET attributes on procedural call handlers. An attacker could use this flaw to cause PostgreSQL to crash, leading to a denial of service. (CVE-2012-2655)

Vulnerability Detection Method

Details: `Ubuntu Update for postgresql-9.1 USN-1461-1`

OID:1.3.6.1.4.1.25623.1.0.841032

Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-2143
cve: CVE-2012-2655
url: http://www.ubuntu.com/usn/usn-1461-1/
usn: 1461-1
cert-bund: CB-K15/1514
dfn-cert: DFN-CERT-2012-1922
dfn-cert: DFN-CERT-2012-1917
dfn-cert: DFN-CERT-2012-1878
dfn-cert: DFN-CERT-2012-1446
dfn-cert: DFN-CERT-2012-1316
dfn-cert: DFN-CERT-2012-1302
dfn-cert: DFN-CERT-2012-1289
dfn-cert: DFN-CERT-2012-1288
dfn-cert: DFN-CERT-2012-1287
dfn-cert: DFN-CERT-2012-1280
dfn-cert: DFN-CERT-2012-1279
dfn-cert: DFN-CERT-2012-1268
dfn-cert: DFN-CERT-2012-1266
dfn-cert: DFN-CERT-2012-1243
dfn-cert: DFN-CERT-2012-1242
dfn-cert: DFN-CERT-2012-1162
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-1159
dfn-cert: DFN-CERT-2012-1148
dfn-cert: DFN-CERT-2012-1107
dfn-cert: DFN-CERT-2012-1035
```

Medium (CVSS: 4.0)
NVT: Ubuntu Update for gnutls26 USN-1752-1

Summary
The remote host is missing an update for the 'gnutls26' package(s) announced via the referenced advisory.

Vulnerability Detection Result

```
Vulnerable package: libgnutls13
Installed version:  2.0.4-1ubuntu2
Fixed version:      2.0.4-1ubuntu2.9
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
gnutls26 on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Nadhem Alfardan and Kenny Paterson discovered that the TLS protocol as used in GnuTLS was vulnerable to a timing side-channel attack known as the 'Lucky Thirteen' issue. A remote attacker could use this issue to perform plaintext-recovery attacks via analysis of timing data.

Vulnerability Detection Method
Details: `Ubuntu Update for gnutls26 USN-1752-1`
OID:1.3.6.1.4.1.25623.1.0.841340
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2013-1619
url: http://www.ubuntu.com/usn/usn-1752-1/
usn: 1752-1
cert-bund: CB-K14/0262
cert-bund: CB-K14/0255
cert-bund: CB-K13/0093
dfn-cert: DFN-CERT-2014-0264
dfn-cert: DFN-CERT-2014-0262
dfn-cert: DFN-CERT-2013-1004
dfn-cert: DFN-CERT-2013-0927
dfn-cert: DFN-CERT-2013-0551
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2013-0550
dfn-cert: DFN-CERT-2013-0546
dfn-cert: DFN-CERT-2013-0486
dfn-cert: DFN-CERT-2013-0471
dfn-cert: DFN-CERT-2013-0317
```

[return to 10.0.3.5]

2.1.3 Low general/tcp

Low (CVSS: 3.3)
NVT: Ubuntu Update for fuse vulnerabilities USN-1077-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1077-1

Vulnerability Detection Result

```
Vulnerable package: fuse-utils
Installed version:  2.7.2-1ubuntu2
Fixed version:      2.7.2-1ubuntu2.3
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
fuse vulnerabilities on Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight
It was discovered that FUSE would incorrectly follow symlinks when checking mountpoints under certain conditions. A local attacker, with access to use FUSE, could unmount arbitrary locations, leading to a denial of service.

Vulnerability Detection Method
Details: `Ubuntu Update for fuse vulnerabilities USN-1077-1`
OID:1.3.6.1.4.1.25623.1.0.840606
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2009-3297
cve: CVE-2011-0541
cve: CVE-2011-0542
cve: CVE-2011-0543
url: http://www.ubuntu.com/usn/usn-1077-1/
usn: 1077-1
dfn-cert: DFN-CERT-2011-1093
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-0492
dfn-cert: DFN-CERT-2010-0639
dfn-cert: DFN-CERT-2010-0275
dfn-cert: DFN-CERT-2010-0268
dfn-cert: DFN-CERT-2010-0266
dfn-cert: DFN-CERT-2010-0218
dfn-cert: DFN-CERT-2010-0198
dfn-cert: DFN-CERT-2010-0155
dfn-cert: DFN-CERT-2010-0136
dfn-cert: DFN-CERT-2010-0134
dfn-cert: DFN-CERT-2010-0133
dfn-cert: DFN-CERT-2010-0129
```

Low (CVSS: 2.6)
NVT: Ubuntu Update for apache2 USN-1627-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1627-1

Vulnerability Detection Result

```
Vulnerable package: apache2.2-common
Installed version:  2.2.8-1ubuntu0.15
Fixed version:      2.2.8-1ubuntu0.24
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
apache2 on Ubuntu 12.10, Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that the mod_negotiation module incorrectly handled certain filenames, which could result in browsers becoming vulnerable to cross-site scripting attacks when processing the output. With cross-site scripting vulnerabilities, if a user were tricked into viewing server output during a crafted server request, a remote attacker could exploit this to modify the contents, or steal confidential data (such as passwords), within the same domain. (CVE-2012-2687)
It was discovered that the Apache HTTP Server was vulnerable to the 'CRIME' SSL data compression attack. Although this issue had been mitigated on the client with newer web browsers, this update also disables SSL data compression on the server. A new SSLCompression directive for Apache has been backported that may be used to re-enable SSL data compression in certain environments. (CVE-2012-4929)

Vulnerability Detection Method
Details: `Ubuntu Update for apache2 USN-1627-1`
OID:1.3.6.1.4.1.25623.1.0.841209

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2019-03-13T09:25:59Z

References

cve: CVE-2012-2687
cve: CVE-2012-4929
url: http://www.ubuntu.com/usn/usn-1627-1/
usn: 1627-1
url: http://httpd.apache.org/docs/2.4/mod/mod_ssl.html
cert-bund: CB-K17/0504
cert-bund: CB-K15/0960
cert-bund: CB-K15/0637
cert-bund: CB-K14/1568
cert-bund: CB-K14/1531
cert-bund: CB-K14/1342
cert-bund: CB-K14/0458
cert-bund: CB-K13/0882
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2015-1008
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2014-1668
dfn-cert: DFN-CERT-2014-1644
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-0483
dfn-cert: DFN-CERT-2013-1893
dfn-cert: DFN-CERT-2013-1307
dfn-cert: DFN-CERT-2013-0716
dfn-cert: DFN-CERT-2013-0672
dfn-cert: DFN-CERT-2013-0631
dfn-cert: DFN-CERT-2013-0469
dfn-cert: DFN-CERT-2013-0342
dfn-cert: DFN-CERT-2013-0324
dfn-cert: DFN-CERT-2013-0321
dfn-cert: DFN-CERT-2013-0270
dfn-cert: DFN-CERT-2013-0237
dfn-cert: DFN-CERT-2013-0234
dfn-cert: DFN-CERT-2013-0112
dfn-cert: DFN-CERT-2013-0040
dfn-cert: DFN-CERT-2012-2277
dfn-cert: DFN-CERT-2012-2191
dfn-cert: DFN-CERT-2012-2062
dfn-cert: DFN-CERT-2012-1973
dfn-cert: DFN-CERT-2012-1966

Low (CVSS: 2.6)
NVT: Ubuntu Update for apt USN-1477-1

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Ubuntu Update for Linux kernel vulnerabilities USN-1477-1

Vulnerability Detection Result

```
Vulnerable package: apt
Installed version:  0.7.9ubuntu17
Fixed version:      0.7.9ubuntu17.6
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

apt on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight

Georgi Guninski discovered that APT did not properly validate imported keyrings via apt-key net-update. USN-1475-1 added additional verification for imported keyrings, but it was insufficient. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to install altered packages. This update corrects the issue by disabling the net-update option completely. A future update will re-enable the option with corrected verification.

Vulnerability Detection Method

Details: `Ubuntu Update for apt USN-1477-1`
OID:1.3.6.1.4.1.25623.1.0.841045
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2012-0954
url: http://www.ubuntu.com/usn/usn-1477-1/
usn: 1477-1
```

Low (CVSS: 2.6)
NVT: Ubuntu Update for apt USN-1475-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1475-1

Vulnerability Detection Result

```
Vulnerable package: apt
Installed version:  0.7.9ubuntu17
Fixed version:      0.7.9ubuntu17.5
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
apt on Ubuntu 12.04 LTS, Ubuntu 11.10, Ubuntu 11.04, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
Georgi Guninski discovered that APT relied on GnuPG argument order and did not check GPG subkeys when validating imported keyrings via apt-key net-update. While it appears that a man-in-the-middle attacker cannot exploit this, as a hardening measure this update adjusts apt-key to validate all subkeys when checking for key collisions.

Vulnerability Detection Method
Details: `Ubuntu Update for apt USN-1475-1`
OID:1.3.6.1.4.1.25623.1.0.841037
Version used: `2019-03-13T09:25:59Z`

References
```
cve: CVE-2012-0954
cve: CVE-2012-3587
url: http://www.ubuntu.com/usn/usn-1475-1/
usn: 1475-1
```

Low (CVSS: 2.6)
NVT: Ubuntu Update for apt USN-1283-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1283-1

Vulnerability Detection Result
```
Vulnerable package: apt
Installed version:  0.7.9ubuntu17
Fixed version:      0.7.9ubuntu17.4
```

Solution
Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS
apt on Ubuntu 11.04, Ubuntu 10.10, Ubuntu 10.04 LTS, Ubuntu 8.04 LTS

Vulnerability Insight
It was discovered that APT incorrectly handled the Verify-Host configuration option. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to steal repository credentials. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2011-3634)

. . . continues on next page . . .

. . . continued from previous page . . .

USN-1215-1 fixed a vulnerability in APT by disabling the apt-key net-update option. This update re-enables the option with corrected verification. Original advisory details: It was discovered that the apt-key utility incorrectly verified GPG keys when downloaded via the net-update option. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to install altered packages.

Vulnerability Detection Method

Details: `Ubuntu Update for apt USN-1283-1`
OID:1.3.6.1.4.1.25623.1.0.840825
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2011-3634
url: http://www.ubuntu.com/usn/usn-1283-1/
usn: 1283-1
```

Low (CVSS: 2.1)
NVT: Ubuntu Update for dbus vulnerability USN-1044-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1044-1

Vulnerability Detection Result

```
Vulnerable package: libdbus-1-3
Installed version:  1.1.20-1ubuntu1
Fixed version:      1.1.20-1ubuntu3.4
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

dbus vulnerability on Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10

Vulnerability Insight

Remi Denis-Courmont discovered that D-Bus did not properly validate the number of nested variants when validating D-Bus messages. A local attacker could exploit this to cause a denial of service.

Vulnerability Detection Method

Details: `Ubuntu Update for dbus vulnerability USN-1044-1`
OID:1.3.6.1.4.1.25623.1.0.840570
Version used: `2019-03-13T09:25:59Z`

References

```
cve: CVE-2010-4352
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.ubuntu.com/usn/usn-1044-1/
usn: 1044-1
cert-bund: CB-K15/1514
dfn-cert: DFN-CERT-2012-2063
dfn-cert: DFN-CERT-2011-0712
dfn-cert: DFN-CERT-2011-0565
dfn-cert: DFN-CERT-2011-0431
dfn-cert: DFN-CERT-2011-0244
dfn-cert: DFN-CERT-2011-0088
dfn-cert: DFN-CERT-2010-1759
```

[return to 10.0.3.5]

This file was automatically generated.