Scan Report

September 18, 2023

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 “Assignment1”. The scan started at Sun Aug 27 21:28:48 2023 UTC and ended at Sun Aug 27 21:51:07 2023 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
10.2.2.100	56	94	10	0	0
Total: 1	56	94	10	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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.
It only lists hosts that produced issues.
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 160 results selected by the filtering described above. Before filtering there were 1031 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.2.2.100	SSH	Success	Protocol SSH, Port 22, User root
10.2.2.100	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 10.2.2.100

Host scan start Sun Aug 27 21:29:09 2023 UTC
Host scan end Sun Aug 27 21:51:06 2023 UTC

Service (Port)	Threat Level
21/tcp	High
8787/tcp	High
5432/tcp	High
512/tcp	High
6200/tcp	High
3632/tcp	High
514/tcp	High
513/tcp	High
general/tcp	High

. . . (continues) . . .

. . . (continued) . . .

Service (Port)	Threat Level
22/tcp	High
1524/tcp	High
80/tcp	High
3306/tcp	High
21/tcp	Medium
5432/tcp	Medium
23/tcp	Medium
general/tcp	Medium
22/tcp	Medium
25/tcp	Medium
445/tcp	Medium
80/tcp	Medium
general/tcp	Low
22/tcp	Low
80/tcp	Low

2.1.1 High 21/tcp

High (CVSS: 7.5)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary
vsftpd is prone to a backdoor vulnerability.

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

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution
Solution type: VendorFix
The repaired package can be downloaded from the referenced link. Please validate the package with its signature.

Affected Software/OS
The vsftpd 2.3.4 source package is affected.

Vulnerability Detection Method
Details: `vsftpd Compromised Source Packages Backdoor Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: `$Revision: 12076 $`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
BID:48539
Other:
  URL:http://www.securityfocus.com/bid/48539
   URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back
↪doored.html
   URL:https://security.appspot.com/vsftpd.html
```

[return to 10.2.2.100]

2.1.2 High 8787/tcp

High (CVSS: 10.0)
NVT: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities

Summary
Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.

Vulnerability Detection Result

```
The service is running in $SAFE >= 1 mode. However it is still possible to run a
↪rbitrary syscall commands on the remote host. Sending an invalid syscall the s
↪ervice returned the following response:
Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in ‘syscall’"0/usr/lib/
↪ruby/1.8/drb/drb.rb:1555:in ‘send’"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in ‘__se
↪nd__’"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in ‘perform_without_block’"3/usr/lib/
↪ruby/1.8/drb/drb.rb:1515:in ‘perform’"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in ‘m
↪ain_loop’"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in ‘loop’"5/usr/lib/ruby/1.8/drb/
↪drb.rb:1585:in ‘main_loop’"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in ‘start’"5/usr
↪/lib/ruby/1.8/drb/drb.rb:1581:in ‘main_loop’"//usr/lib/ruby/1.8/drb/drb.rb:143
↪0:in ‘run’"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in ‘start’"//usr/lib/ruby/1.8/dr
↪b/drb.rb:1427:in ‘run’"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in ‘initialize’"//us
↪r/lib/ruby/1.8/drb/drb.rb:1627:in ‘new’"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in
↪‘start_service’"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not im
↪plemented
```

Impact
By default, Distributed Ruby does not impose restrictions on allowed hosts or set the $SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.

Solution
Solution type: Mitigation
Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:

. . . continues on next page . . .

. . . continued from previous page . . .

- Implementing taint on untrusted input
- Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate)
- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts

Vulnerability Detection Method
Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.
Details: `Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.108010
Version used: `$Revision: 12338 $`

References

```
BID:47071
Other:
  URL:https://tools.cisco.com/security/center/viewAlert.x?alertId=22750
   URL:http://www.securityfocus.com/bid/47071
   URL:http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_t
↪esters/
   URL:http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html
```

[return to 10.2.2.100]

2.1.3 High 5432/tcp

High (CVSS: 9.0)
NVT: PostgreSQL weak password

Summary
It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

Vulnerability Detection Result

```
It was possible to login as user postgres with password "postgres".
```

Solution
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Details: `PostgreSQL weak password`
OID:1.3.6.1.4.1.25623.1.0.103552
Version used: `$Revision: 10312 $`

[return to 10.2.2.100]

2.1.4 High 512/tcp

High (CVSS: 10.0)
NVT: rexec Passwordless / Unencrypted Cleartext Login

Summary
This remote host is running a rexec service.

Vulnerability Detection Result

```
The rexec service is not allowing connections from this host.
```

Solution
Solution type: Mitigation
Disable the rexec service and use alternatives like SSH instead.

Vulnerability Insight
rexec (Remote Process Execution) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer.
The main difference is that rexec authenticate by reading the username and password *unencrypted* from the socket.

Vulnerability Detection Method
Details: `rexec Passwordless / Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.100111
Version used: `$Revision: 13541 $`

References

```
Other:
  URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0618
```

[return to 10.2.2.100]

2.1.5 High 6200/tcp

High (CVSS: 7.5)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary
vsftpd is prone to a backdoor vulnerability.

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

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application.
Successful attacks will compromise the affected application.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix

The repaired package can be downloaded from the referenced link. Please validate the package with its signature.

Affected Software/OS

The vsftpd 2.3.4 source package is affected.

Vulnerability Detection Method

Details: `vsftpd Compromised Source Packages Backdoor Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.103185

Version used: `$Revision: 12076 $`

References

```
BID:48539
Other:
  URL:http://www.securityfocus.com/bid/48539
   URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back
↪doored.html
   URL:https://security.appspot.com/vsftpd.html
```

[return to 10.2.2.100]

2.1.6 High 3632/tcp

High (CVSS: 9.3)

NVT: DistCC Remote Code Execution Vulnerability

Summary

DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

Vulnerability Detection Result

```
It was possible to execute the "id" command.
Result: uid=1(daemon) gid=1(daemon)
```

Impact

DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.

Solution

Solution type: VendorFix

Vendor updates are available. Please see the references for more information.

For more information about DistCC's security see the references.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Details: `DistCC Remote Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103553
Version used: `$Revision: 12032 $`

References

```
CVE: CVE-2004-2687
Other:
  URL:https://distcc.github.io/security.html
   URL:https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:
↪80/archives/bugtraq/2005-03/0183.html
```

[return to 10.2.2.100]

2.1.7 High 514/tcp

High (CVSS: 7.5)
NVT: rsh Unencrypted Cleartext Login

Summary
This remote host is running a rsh service.

Vulnerability Detection Result

```
The rsh service currently has issues with name resolution and is not allowing co
↪nnections from this host.
```

Solution
Solution type: Mitigation
Disable the rsh service and use alternatives like SSH instead.

Vulnerability Insight
rsh (remote shell) is a command line computer program which can execute shell commands as another user, and on another computer across a computer network.

Vulnerability Detection Method
Details: `rsh Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.100080
Version used: `$Revision: 13010 $`

References

```
Other:
  URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651
```

[return to 10.2.2.100]

2.1.8 High 513/tcp

High (CVSS: 7.5)
NVT: rlogin Passwordless / Unencrypted Cleartext Login

Summary
This remote host is running a rlogin service.

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

Solution
Solution type: Mitigation
Disable the rlogin service and use alternatives like SSH instead.

Vulnerability Insight
rlogin has several serious security problems,
- all information, including passwords, is transmitted unencrypted.
- .rlogin (or .rhosts) file is easy to misuse (potentially allowing anyone to login without a password)

Vulnerability Detection Method
Details: `rlogin Passwordless / Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.901202
Version used: `$Revision: 13541 $`

References
```
Other:
  URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651
   URL:http://en.wikipedia.org/wiki/Rlogin
   URL:http://www.ietf.org/rfc/rfc1282.txt
```

[return to 10.2.2.100]

2.1.9 High general/tcp

High (CVSS: 10.0)
NVT: TightVNC ClientConnection Multiple Integer Overflow Vulnerabilities (Linux)

Summary
This host is running TightVNC and is prone to Multiple Integer Overflow Vulnerability.

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

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will let the attacker execute arbitrary codes in the context of the application and may cause remote code execution to compromise the affected remote system.

Solution
Solution type: VendorFix
Upgrade to the latest version 1.3.10.

Affected Software/OS
TightVNC version 1.3.9 and prior on Linux.

Vulnerability Insight
Multiple Integer Overflow due to signedness errors within the functions ClientConnection::CheckBufferSize and ClientConnection::CheckFileZipBufferSize in ClientConnection.cpp file fails to validate user input.

Vulnerability Detection Method
Details: `TightVNC ClientConnection Multiple Integer Overflow Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900475
Version used: `2019-04-29T15:08:03+0000`

References

```
CVE: CVE-2009-0388
BID:33568
Other:
  URL:http://milw0rm.com/exploits/7990
   URL:http://milw0rm.com/exploits/8024
   URL:http://www.coresecurity.com/content/vnc-integer-overflows
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 12670 $`

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-2009-2694
BID:36071
Other:
  URL:http://secunia.com/advisories/36384
   URL:http://www.pidgin.im/news/security/?id=34
   URL:http://www.vupen.com/english/advisories/2009/2303
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-1182
Other:
  URL:http://www.ubuntu.com/usn/usn-1423-1/
   USN:1423-1
```

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

Vulnerability Detection Method

Details: `OS End Of Life Detection`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.103674
Version used: $Revision: 8927 $

Product Detection Result
Product: cpe:/o:canonical:ubuntu_linux:8.04:-:lts
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 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: $Revision: 14132 $

References

```
Other:
  URL:http://www.ubuntu.com/usn/usn-1215-1/
   USN:1215-1
```

. . . continues on next page . . .

. . . continued from previous page . . .

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)
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)

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-1126, CVE-2012-1127, CVE-2012-1128, CVE-2012-1129, CVE-2012-1130,
↪CVE-2012-1131, CVE-2012-1132, CVE-2012-1133, CVE-2012-1134, CVE-2012-1135, CVE
↪-2012-1136, CVE-2012-1137, CVE-2012-1138, CVE-2012-1139, CVE-2012-1140, CVE-20
↪12-1141, CVE-2012-1142, CVE-2012-1143, CVE-2012-1144
Other:
  URL:http://www.ubuntu.com/usn/usn-1403-1/
   USN:1403-1
```

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.

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 12551 $`

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
Other:
  URL:https://ftp.gnu.org/gnu/bash/
   URL:https://shellshocker.net/
   URL:http://lcamtuf.blogspot.in/2014/09/bash-bug-apply-unofficial-patch-now.ht
↪ml
```

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)
```

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 `='
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
/bin/bash: X: line 1: ‘’
/bin/bash: error importing function definition for ‘X’
uid=0(root) gid=0(root) groups=0(root)
```

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: `$Revision: 12551 $`

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
Other:
  URL:https://ftp.gnu.org/gnu/bash/
   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-co
↪de-execution-vulnerability-cve-2014-6271
```

High (CVSS: 10.0)

NVT: GNU Bash Stacked Redirects aka ’redir_stack’ Memory Corruption Vulnerability (LSC)

. . . 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 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: 32299 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

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: `$Revision: 12551 $`

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-2014-7186
BID:70152
Other:
  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.ht
↪ml
   URL:http://www.gnu.org/software/bash/
```

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

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:   357 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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 12551 $`

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-2014-6277
BID:70165
Other:
  URL:https://shellshocker.net
   URL:http://lcamtuf.blogspot.in/2014/09/bash-bug-apply-unofficial-patch-now.ht
↪ml
   URL:https://ftp.gnu.org/gnu/bash/
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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
Version used: `$Revision: 12551 $`

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
Other:
  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/
   URL:http://www.gnu.org/software/bash/
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-0216, CVE-2011-2821, CVE-2011-2834, CVE-2011-3905, CVE-2011-3919
Other:
  URL:http://www.ubuntu.com/usn/usn-1334-1/
   USN:1334-1
```

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.

. . . 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
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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-1944
Other:
  URL:http://www.ubuntu.com/usn/usn-1153-1/
   USN:1153-1
```

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)

. . . continues on next page . . .

. . . continued from previous page . . .

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 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: `$Revision: 14132 $`

References

```
CVE: CVE-2010-2482, CVE-2010-2483, CVE-2010-2595, CVE-2010-2597, CVE-2010-2598,
↪CVE-2010-2630, CVE-2010-3087, CVE-2011-0191, CVE-2011-0192
Other:
  URL:http://www.ubuntu.com/usn/usn-1085-1/
   USN:1085-1
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-3256, CVE-2011-3439
Other:
  URL:http://www.ubuntu.com/usn/usn-1267-1/
   USN:1267-1
```

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
```

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

. . . continues on next page . . .

... continued from previous page ...

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: `$Revision: 14132 $`

References

CVE: CVE-2010-2482, CVE-2010-2595, CVE-2010-2597, CVE-2010-2598, CVE-2010-2630,
↪CVE-2010-3087, CVE-2011-0191

Other:

URL:http://www.ubuntu.com/usn/usn-1085-2/

... continues on next page ...

... continued from previous page ...

```
USN:1085-2
```

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)
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)

... continues on next page ...

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-1945, CVE-2011-3210, CVE-2011-4108, CVE-2012-0050, CVE-2011-4109,
↪CVE-2011-4354, CVE-2011-4576, CVE-2011-4577, CVE-2011-4619, CVE-2012-0027
Other:
  URL:http://www.ubuntu.com/usn/usn-1357-1/
   USN:1357-1
```

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

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2007-5925, CVE-2008-3963, CVE-2008-4098, CVE-2008-4456, CVE-2008-7247,
↪CVE-2009-2446, CVE-2009-4019, CVE-2009-4030, CVE-2009-4484, CVE-2010-1621, CVE
↪-2010-1626, CVE-2010-1848, CVE-2010-1849, CVE-2010-1850, CVE-2010-2008, CVE-20
↪10-3677, CVE-2010-3678, CVE-2010-3679, CVE-2010-3680, CVE-2010-3681, CVE-2010-
↪3682, CVE-2010-3683, CVE-2010-3833, CVE-2010-3834, CVE-2010-3835, CVE-2010-383
↪6, CVE-2010-3837, CVE-2010-3838, CVE-2010-3839, CVE-2010-3840, CVE-2011-2262,
↪CVE-2012-0075, CVE-2012-0087, CVE-2012-0101, CVE-2012-0102, CVE-2012-0112, CVE
↪-2012-0113, CVE-2012-0114, CVE-2012-0115, CVE-2012-0116
Other:
  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
```

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

. . . continues on next page . . .

... continued from previous page ...

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)
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: `$Revision: 14132 $`

References

```
CVE: CVE-2013-1899, CVE-2013-1900, CVE-2013-1901
Other:
  USN:1789-1
   URL:http://www.ubuntu.com/usn/usn-1789-1/
```

High (CVSS: 7.9)
NVT: Ubuntu Update for linux vulnerabilities USN-1072-1

Summary
Ubuntu Update for Linux kernel vulnerabilities USN-1072-1

Vulnerability Detection Result

```
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)

... continues on next page ...

. . . continued from previous page . . .

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

Details: `Ubuntu Update for linux vulnerabilities USN-1072-1`

OID:1.3.6.1.4.1.25623.1.0.840594

Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2010-0435, CVE-2010-2943, CVE-2010-3296, CVE-2010-3297, CVE-2010-3448,
↪CVE-2010-3698, CVE-2010-3699, CVE-2010-3858, CVE-2010-3859, CVE-2010-3873, CVE
↪-2010-3875, CVE-2010-3876, CVE-2010-3877, CVE-2010-3880, CVE-2010-4072, CVE-20
↪10-4074, CVE-2010-4078, CVE-2010-4079, CVE-2010-4080, CVE-2010-4081, CVE-2010-
↪4083, CVE-2010-4157, CVE-2010-4160, CVE-2010-4248
Other:
  URL:http://www.ubuntu.com/usn/usn-1072-1/
   USN:1072-1
```

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-0870
Other:
  URL:http://www.ubuntu.com/usn/usn-1374-1/
   USN:1374-1
```

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

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-5166
Other:
  URL:http://www.ubuntu.com/usn/usn-1601-1/
   USN:1601-1
```

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

Details: `Ubuntu Update for apache2 USN-1199-1`
OID:1.3.6.1.4.1.25623.1.0.840734
Version used: `$Revision: 14132 $`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
CVE: CVE-2011-3192
Other:
  URL:http://www.ubuntu.com/usn/usn-1199-1/
   USN:1199-1
```

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

Summary
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)

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2010-4075, CVE-2010-4076, CVE-2010-4077, CVE-2010-4158, CVE-2010-4162,
↪CVE-2010-4163, CVE-2010-4164, CVE-2010-4242, CVE-2010-4258, CVE-2010-4346
Other:
  URL:http://www.ubuntu.com/usn/usn-1105-1/
   USN:1105-1
```

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)

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2010-0421, CVE-2011-0020, CVE-2011-0064
Other:
  URL:http://www.ubuntu.com/usn/usn-1082-1/
   USN:1082-1
```

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`
OID:1.3.6.1.4.1.25623.1.0.841369
Version used: `$Revision: 14132 $`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
CVE: CVE-2013-1667
Other:
  URL:http://www.ubuntu.com/usn/usn-1770-1/
   USN:1770-1
```

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

```
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)

. . . 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-1358-2`
OID:1.3.6.1.4.1.25623.1.0.840895
Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2012-0831, CVE-2011-4885, CVE-2012-0830, CVE-2011-4153, CVE-2012-0057,
↪CVE-2012-0788, CVE-2011-0441
Other:
  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
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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-1358-1`
OID:1.3.6.1.4.1.25623.1.0.840891
Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2011-4885, CVE-2012-0830, CVE-2011-4153, CVE-2012-0057, CVE-2012-0788,
↪CVE-2012-0831, CVE-2011-0441
Other:
  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
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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)
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: `$Revision: 14132 $`

References
```
CVE: CVE-2009-5029, CVE-2010-0015, CVE-2011-1071, CVE-2011-1659, CVE-2011-1089,
↪CVE-2011-1095, CVE-2011-1658, CVE-2011-2702, CVE-2011-4609, CVE-2012-0864
Other:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  URL:http://www.ubuntu.com/usn/usn-1396-1/
   USN:1396-1
```

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)
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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-2939, CVE-2011-3597, CVE-2012-5195, CVE-2012-5526
Other:
  URL:http://www.ubuntu.com/usn/usn-1643-1/
   USN:1643-1
```

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-2088, CVE-2012-2113
Other:
  URL:http://www.ubuntu.com/usn/usn-1498-1/
   USN:1498-1
```

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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

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: `$Revision: 14132 $`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2011-1938, CVE-2011-2202, CVE-2011-2483, CVE-2011-3182, CVE-2011-3267,
↪CVE-2011-1657, CVE-2010-1914, CVE-2010-2484
Other:
  URL:http://www.ubuntu.com/usn/usn-1231-1/
   USN:1231-1
```

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`
OID:1.3.6.1.4.1.25623.1.0.840685

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2011-2192, CVE-2010-0734, CVE-2009-2417
Other:
  URL:http://www.ubuntu.com/usn/usn-1158-1/
   USN:1158-1
```

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

```
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)

. . . continues on next page . . .

. . . continued from previous page . . .

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.

Vulnerability Detection Method

Details: `Ubuntu Update for php5 USN-1126-2`

OID:1.3.6.1.4.1.25623.1.0.840636

Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2010-4697, CVE-2011-1072, CVE-2011-1144, CVE-2011-0441, CVE-2010-4698,
↪CVE-2006-7243, CVE-2011-0420, CVE-2011-0421, CVE-2011-0708, CVE-2011-1092, CVE
↪-2011-1148, CVE-2011-1153, CVE-2011-1464, CVE-2011-1466, CVE-2011-1467, CVE-20
↪11-1468, CVE-2011-1469, CVE-2011-1470, CVE-2011-1471
Other:
  URL:http://www.ubuntu.com/usn/usn-1126-2/
   USN:1126-2
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-0997
Other:
  URL:http://www.ubuntu.com/usn/usn-1108-1/
   USN:1108-1
```

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)

. . . continues on next page . . .

. . . continued from previous page . . .

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)
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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-0441, CVE-2011-1072, CVE-2011-1144, CVE-2010-4697, CVE-2010-4698,
↪CVE-2006-7243, CVE-2011-0420, CVE-2011-0421, CVE-2011-0708, CVE-2011-1092, CVE
↪-2011-1148, CVE-2011-1153, CVE-2011-1464, CVE-2011-1466, CVE-2011-1467, CVE-20
↪11-1468, CVE-2011-1469, CVE-2011-1470, CVE-2011-1471
Other:
  URL:http://www.ubuntu.com/usn/usn-1126-1/
   USN:1126-1
```

High (CVSS: 7.5)
NVT: Ubuntu Update for libpng USN-1367-1

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2009-5063, CVE-2011-3026
Other:
  URL:http://www.ubuntu.com/usn/usn-1367-1/
   USN:1367-1
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-2311, CVE-2012-1823
Other:
  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
```

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
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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-2337
Other:
  URL:http://www.ubuntu.com/usn/usn-1442-1/
   USN:1442-1
```

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

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)

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2010-3847, CVE-2010-3856
Other:
  URL:http://www.ubuntu.com/usn/usn-1009-2/
   USN:1009-2
```

[return to 10.2.2.100]

2.1.10 High 22/tcp

High (CVSS: 7.5)
NVT: SSH Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote SSH server using default credentials.
As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result

```
It was possible to login with the following credentials <User>:<Password>
msfadmin:msfadmin
user:user
```

Solution
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Try to login with a number of known default credentials via the SSH protocol.
Details: `SSH Brute Force Logins With Default Credentials Reporting`
OID:1.3.6.1.4.1.25623.1.0.103239
Version used: `$Revision: 13568 $`

[return to 10.2.2.100]

2.1.11 High 1524/tcp

High (CVSS: 10.0)
NVT: Possible Backdoor: Ingreslock

Summary
A backdoor is installed on the remote host

Vulnerability Detection Result

```
The service is answering to an 'id;' command with the following response: uid=0(
↪root) gid=0(root)
```

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.

Solution
Solution type: Workaround

Vulnerability Detection Method
Details: `Possible Backdoor: Ingreslock`
OID:1.3.6.1.4.1.25623.1.0.103549
Version used: `$Revision: 11327 $`

[return to 10.2.2.100]

2.1.12 High 80/tcp

High (CVSS: 10.0)
NVT: TWiki XSS and Command Execution Vulnerabilities

Product detection result

```
cpe:/a:twiki:twiki:01.Feb.2003
Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)
```

Summary
The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Vulnerability Detection Result

```
Installed version: 01.Feb.2003
Fixed version:     4.2.4
```

Impact
Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Upgrade to version 4.2.4 or later.

Affected Software/OS
TWiki, TWiki version prior to 4.2.4.

Vulnerability Insight
The flaws are due to,
- %URLPARAM}}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack.
- %SEARCH}}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Vulnerability Detection Method
Details: `TWiki XSS and Command Execution Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.800320
Version used: `$Revision: 12952 $`

Product Detection Result
Product: `cpe:/a:twiki:twiki:01.Feb.2003`
Method: `TWiki Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
```
CVE: CVE-2008-5304, CVE-2008-5305
BID:32668, 32669
Other:
  URL:http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304
   URL:http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305
```

High (CVSS: 7.5)
NVT: Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities

Product detection result
```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

Summary
Tiki Wiki CMS Groupware is prone to multiple unspecified vulnerabilities, including:
- An unspecified SQL-injection vulnerability
- An unspecified authentication-bypass vulnerability
- An unspecified vulnerability

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 1.9.5
Fixed version:     4.2
```

Impact

Exploiting these issues could allow an attacker to compromise the application, access or modify data, exploit latent vulnerabilities in the underlying database, and gain unauthorized access to the affected application. Other attacks are also possible.

Solution

Solution type: VendorFix

The vendor has released an advisory and fixes. Please see the references for details.

Affected Software/OS

Versions prior to Tiki Wiki CMS Groupware 4.2 are vulnerable.

Vulnerability Detection Method

Details: `Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.100537
Version used: `$Revision: 13960 $`

Product Detection Result

Product: `cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`
Method: `Tiki Wiki CMS Groupware Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.901001)

References

```
CVE: CVE-2010-1135, CVE-2010-1134, CVE-2010-1133, CVE-2010-1136
BID:38608
Other:
  URL:http://www.securityfocus.com/bid/38608
   URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=247
↪34
   URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=250
↪46
   URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254
↪24
   URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254
↪35
   URL:http://info.tikiwiki.org/article86-Tiki-Announces-3-5-and-4-2-Releases
   URL:http://info.tikiwiki.org/tiki-index.php?page=homepage
```

High (CVSS: 7.5)
NVT: phpinfo() output Reporting

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.

Vulnerability Detection Result

```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
http://10.2.2.100/mutillidae/phpinfo.php
http://10.2.2.100/phpinfo.php
```

Impact

Some of the information that can be gathered from this file includes:
The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.

Solution

Solution type: Workaround
Delete the listed files or restrict access to them.

Vulnerability Detection Method

Details: `phpinfo() output Reporting`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `$Revision: 11992 $`

High (CVSS: 7.5)
NVT: Test HTTP dangerous methods

Summary

Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.
This script checks if they are enabled and can be misused to upload or delete files.

Vulnerability Detection Result

```
We could upload the following files via the PUT method at this web server:
http://10.2.2.100/dav/puttest700777384.html
We could delete the following files via the DELETE method at this web server:
http://10.2.2.100/dav/puttest700777384.html
```

Impact

- Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server.
- Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

Solution

Solution type: Mitigation

. . . continues on next page . . .

. . . continued from previous page . . .

Use access restrictions to these dangerous HTTP methods or disable them completely.

Vulnerability Detection Method
Details: `Test HTTP dangerous methods`
OID:1.3.6.1.4.1.25623.1.0.10498
Version used: `2019-04-24T07:26:10+0000`

References

```
BID:12141
Other:
  OWASP:OWASP-CM-001
```

High (CVSS: 7.5)
NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.

Summary
PHP is prone to an information-disclosure vulnerability.

Vulnerability Detection Result

```
Vulnerable url: http://10.2.2.100/cgi-bin/php
```

Impact
Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer. Other attacks are also possible.

Solution
Solution type: VendorFix
PHP has released version 5.4.3 and 5.3.13 to address this vulnerability. PHP is recommending that users upgrade to the latest version of PHP.

Vulnerability Insight
When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution.
An example of the -s command, allowing an attacker to view the source code of index.php is below:
http://example.com/index.php?-s

Vulnerability Detection Method
Details: `PHP-CGI-based setups vulnerability when parsing query string parameters from ph.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.103482
Version used: `$Revision: 13679 $`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335
BID:53388
Other:
  URL:http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-r
↪isks-Update-1567532.html
   URL:http://www.kb.cert.org/vuls/id/520827
   URL:http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
   URL:https://bugs.php.net/bug.php?id=61910
   URL:http://www.php.net/manual/en/security.cgi-bin.php
   URL:http://www.securityfocus.com/bid/53388
```

[return to 10.2.2.100]

2.1.13 High 3306/tcp

High (CVSS: 9.0)
NVT: MySQL / MariaDB weak password

Product detection result

```
cpe:/a:mysql:mysql:5.0.51a
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
```

Summary

It was possible to login into the remote MySQL as root using weak credentials.

Vulnerability Detection Result

```
It was possible to login as root with an empty password.
```

Solution

Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method

Details: `MySQL / MariaDB weak password`
OID:1.3.6.1.4.1.25623.1.0.103551
Version used: `$Revision: 12175 $`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.0.51a`
Method: `MySQL/MariaDB Detection`
OID: 1.3.6.1.4.1.25623.1.0.100152)

[return to 10.2.2.100]

2.1.14 Medium 21/tcp

Medium (CVSS: 6.4)
NVT: Anonymous FTP Login Reporting

Summary
Reports if the remote FTP Server allows anonymous logins.

Vulnerability Detection Result

```
It was possible to login to the remote FTP service with the following anonymous
↪account(s):
anonymous:anonymous@example.com
ftp:anonymous@example.com
```

Impact
Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:
- gain access to sensitive files
- upload or delete files.

Solution
Solution type: Mitigation
If you do not want to share files, you should disable anonymous logins.

Vulnerability Insight
A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

Vulnerability Detection Method
Details: `Anonymous FTP Login Reporting`
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: `$Revision: 12030 $`

References
```
Other:
  URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497
```

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Anonymous sessions:     331 Please specify the password.
Non-anonymous sessions: 331 Please specify the password.
```

Impact

An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution

Solution type: Mitigation

Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.

Details: `FTP Unencrypted Cleartext Login`

OID:1.3.6.1.4.1.25623.1.0.108528

Version used: `$Revision: 13611 $`

[return to 10.2.2.100]

2.1.15 Medium 5432/tcp

Medium (CVSS: 6.8)
NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

Summary

OpenSSL is prone to security-bypass vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.

Solution

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Vulnerability Detection Method

Send two SSL ChangeCipherSpec request and check the response.
Details: `SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105042
Version used: `$Revision: 12865 $`

References

```
CVE: CVE-2014-0224
BID:67899
Other:
  URL:https://www.openssl.org/news/secadv/20140605.txt
   URL:http://www.securityfocus.com/bid/67899
   URL:http://openssl.org/
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary

The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result

```
The certificate of the remote service expired on 2010-04-16 14:07:45.
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
subject alternative names (SAN):
None
issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: Mitigation

Replace the SSL/TLS certificate by a new one.

Vulnerability Insight

This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method

Details: `SSL/TLS: Certificate Expired`

OID:1.3.6.1.4.1.25623.1.0.103955

Version used: `$Revision: 11103 $`

Medium (CVSS: 4.3)

NVT: SSL/TLS: Report Weak Cipher Suites

Summary

This routine reports all Weak SSL/TLS cipher suites accepted by a service.

NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_SHA
```

Solution

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

Please see the references for more resources supporting you with this task.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:

- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method

Details: `SSL/TLS: Report Weak Cipher Suites`

OID:1.3.6.1.4.1.25623.1.0.103440

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 11135 $`

References

```
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
  URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-
↪1465_update_6.html
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Summary

This host is prone to an information disclosure vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

Solution

Solution type: Mitigation

Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight

The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method

Evaluate previous collected information about this service.

Details: `SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.802087

Version used: `$Revision: 11402 $`

References

```
CVE: CVE-2014-3566
BID:70574
Other:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  URL:https://www.openssl.org/~bodo/ssl-poodle.pdf
   URL:https://www.imperialviolet.org/2014/10/14/poodle.html
   URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
   URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit
↪ing-ssl-30.html
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Summary
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.8
↪02067) NVT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Solution
Solution type: Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

Vulnerability Insight
The SSLv2 and SSLv3 protocols containing known cryptographic flaws like:
- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)
- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

Vulnerability Detection Method
Check the used protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `$Revision: 5547 $`

References

```
CVE: CVE-2016-0800, CVE-2014-3566
Other:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/delivera
↪bles/algorithms-key-sizes-and-parameters-report
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
   URL:https://drownattack.com/
   URL:https://www.imperialviolet.org/2014/10/14/poodle.html
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173
↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic
↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi
↪ng outside US,C=XX
Signature Algorithm:  sha1WithRSAEncryption
```

Solution
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1,Fingerprint2

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `$Revision: 11524 $`

References

```
Other:
  URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with
↪-sha-1-based-signature-algorithms/
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

```
Server Temporary Key Size: 1024 bits
```

Impact

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution

Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method

Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `$Revision: 12865 $`

References

```
Other:
  URL:https://weakdh.org/
   URL:https://weakdh.org/sysadmin.html
```

[return to 10.2.2.100]

2.1.16 Medium 23/tcp

Medium (CVSS: 4.8)
NVT: Telnet Unencrypted Cleartext Login

Summary
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

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

Impact
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

Solution
Solution type: Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

Vulnerability Detection Method
Details: `Telnet Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108522
Version used: `$Revision: 13620 $`

[return to 10.2.2.100]

2.1.17 Medium general/tcp

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.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

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

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: `$Revision: 14132 $`

References

```
CVE: CVE-2009-0887, CVE-2010-3316, CVE-2010-3430, CVE-2010-3431, CVE-2010-3435,
↪CVE-2010-3853, CVE-2010-4706, CVE-2010-4707
Other:
  URL:http://www.ubuntu.com/usn/usn-1140-1/
   USN:1140-1
```

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

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1576-1

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-3524
Other:
  URL:http://www.ubuntu.com/usn/usn-1576-1/
   USN:1576-1
```

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)

. . . continues on next page . . .

. . . continued from previous page . . .

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)
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: `$Revision: 14132 $`

References

```
CVE: CVE-2008-5983, CVE-2010-1634, CVE-2010-2089, CVE-2010-3493, CVE-2011-1015,
↪CVE-2011-1521, CVE-2011-4940, CVE-2011-4944, CVE-2012-0845, CVE-2012-0876, CVE
↪-2012-1148
Other:
  URL:http://www.ubuntu.com/usn/usn-1613-1/
   USN:1613-1
```

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2009-2939, CVE-2011-0411
Other:
  URL:http://www.ubuntu.com/usn/usn-1113-1/
   USN:1113-1
```

Medium (CVSS: 6.9)

NVT: Ubuntu Update for sudo USN-1754-1

Summary

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2013-1775
Other:
  URL:http://www.ubuntu.com/usn/usn-1754-1/
   USN:1754-1
```

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)

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-1098, CVE-2011-1154, CVE-2011-1155, CVE-2011-1548
Other:
  URL:http://www.ubuntu.com/usn/usn-1172-1/
   USN:1172-1
```

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)

. . . continues on next page . . .

. . . continued from previous page . . .

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-1140-2`
OID:1.3.6.1.4.1.25623.1.0.840673
Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2009-0887, CVE-2010-3316, CVE-2010-3430, CVE-2010-3431, CVE-2010-3435,
↪CVE-2010-3853, CVE-2010-4706, CVE-2010-4707
Other:
  URL:http://www.ubuntu.com/usn/usn-1140-2/
   USN:1140-2
```

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)

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-3148, CVE-2011-3149, CVE-2011-3628
Other:
  URL:http://www.ubuntu.com/usn/usn-1237-1/
   USN:1237-1
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Ubuntu Update for dbus USN-1576-2`
OID:1.3.6.1.4.1.25623.1.0.841177
Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2012-3524
Other:
  URL:http://www.ubuntu.com/usn/usn-1576-2/
   USN:1576-2
```

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

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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-3048
Other:
  URL:http://www.ubuntu.com/usn/usn-1417-1/
   USN:1417-1
```

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
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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-1167
Other:
  URL:http://www.ubuntu.com/usn/usn-1102-1/
   USN:1102-1
```

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

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 derefence 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: `$Revision: 14132 $`

References

```
CVE: CVE-2009-5016, CVE-2010-3436, CVE-2010-3709, CVE-2010-3710, CVE-2010-3870,
↪CVE-2010-4156, CVE-2010-4409, CVE-2010-4645
Other:
  URL:http://www.ubuntu.com/usn/usn-1042-1/
   USN:1042-1
```

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)
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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-1024, CVE-2011-1025, CVE-2011-1081
Other:
  URL:http://www.ubuntu.com/usn/usn-1100-1/
   USN:1100-1
```

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-1173, CVE-2010-4665
Other:
  URL:http://www.ubuntu.com/usn/usn-1416-1/
   USN:1416-1
```

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

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
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: `$Revision: 14132 $`

References
```
CVE: CVE-2012-5581
Other:
  URL:http://www.ubuntu.com/usn/usn-1655-1/
   USN:1655-1
```

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
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2013-0255
Other:
  URL:http://www.ubuntu.com/usn/usn-1717-1/
   USN:1717-1
```

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

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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-1720
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Other:
  URL:http://www.ubuntu.com/usn/usn-1131-1/
   USN:1131-1
```

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

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-0866, CVE-2012-0867, CVE-2012-0868
Other:
  URL:http://www.ubuntu.com/usn/usn-1378-1/
   USN:1378-1
```

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
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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-3102
Other:
  URL:http://www.ubuntu.com/usn/usn-1447-1/
   USN:1447-1
```

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-5134
Other:
  URL:http://www.ubuntu.com/usn/usn-1656-1/
   USN:1656-1
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-3404, CVE-2012-3405, CVE-2012-3406, CVE-2012-3480
Other:
  URL:http://www.ubuntu.com/usn/usn-1589-2/
   USN:1589-2
```

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
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)

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Details: `Ubuntu Update for openssl USN-1451-1`
OID:1.3.6.1.4.1.25623.1.0.841013
Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2012-0884, CVE-2012-2333
Other:
  URL:http://www.ubuntu.com/usn/usn-1451-1/
   USN:1451-1
```

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.

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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-3045
Other:
  URL:http://www.ubuntu.com/usn/usn-1402-1/
   USN:1402-1
```

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
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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-4447, CVE-2012-4564
Other:
  URL:http://www.ubuntu.com/usn/usn-1631-1/
   USN:1631-1
```

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-2501, CVE-2011-2690, CVE-2011-2692
Other:
  URL:http://www.ubuntu.com/usn/usn-1175-1/
   USN:1175-1
```

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

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: `$Revision: 14132 $`

References

```
Other:
  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

. . . continues on next page . . .

. . . continued from previous page . . .

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)

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-3404, CVE-2012-3405, CVE-2012-3406, CVE-2012-3480
Other:
  URL:http://www.ubuntu.com/usn/usn-1589-1/
   USN:1589-1
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Ubuntu Update for libxml2 USN-1587-1`
OID:1.3.6.1.4.1.25623.1.0.841166
Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2012-2807
Other:
  URL:http://www.ubuntu.com/usn/usn-1587-1/
   USN:1587-1
```

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: `$Revision: 14132 $`

References

```
CVE: CVE-2010-4015
Other:
  URL:http://www.ubuntu.com/usn/usn-1058-1/
   USN:1058-1
```

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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-4566
Other:
  URL:http://www.ubuntu.com/usn/usn-1307-1/
   USN:1307-1
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-3152, CVE-2011-3154
Other:
  URL:http://www.ubuntu.com/usn/usn-1284-2/
   USN:1284-2
```

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.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2010-3879
Other:
  URL:http://www.ubuntu.com/usn/usn-1045-2/
   USN:1045-2
```

Medium (CVSS: 5.8)
NVT: Ubuntu Update for fuse vulnerability USN-1045-1

Summary

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`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.840568
Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2010-3879
Other:
  URL:http://www.ubuntu.com/usn/usn-1045-1/
   USN:1045-1
```

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

Summary

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-6085
Other:
  URL:http://www.ubuntu.com/usn/usn-1682-1/
   USN:1682-1
```

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
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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-2122
Other:
  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
```

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-0841
Other:
  URL:http://www.ubuntu.com/usn/usn-1376-1/
   USN:1376-1
```

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

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1527-1

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-0876, CVE-2012-1148
Other:
  URL:http://www.ubuntu.com/usn/usn-1527-1/
   USN:1527-1
```

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)

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-4128, CVE-2012-1573
Other:
  URL:http://www.ubuntu.com/usn/usn-1418-1/
   USN:1418-1
```

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
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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-0719
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Other:
  URL:http://www.ubuntu.com/usn/usn-1075-1/
   USN:1075-1
```

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
Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2010-3436
Other:
  URL:http://www.ubuntu.com/usn/usn-1042-2/
   USN:1042-2
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

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: `$Revision: 12670 $`

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
Other:
  URL:http://www.openwall.com/lists/oss-security/2010/01/07/2
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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
```

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: `$Revision: 12670 $`

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
Other:
  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
```

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
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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-3368, CVE-2011-3348, CVE-2011-1176
Other:
  URL:http://www.ubuntu.com/usn/usn-1259-1/
   USN:1259-1
```

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
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: `$Revision: 14132 $`

References

```
CVE: CVE-2013-1944
Other:
  USN:1801-1
   URL:http://www.ubuntu.com/usn/usn-1801-1/
```

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix

Please Install the Updated Packages.

Affected Software/OS

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-1569
Other:
  URL:http://www.ubuntu.com/usn/usn-1436-1/
   USN:1436-1
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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)

Vulnerability Detection Method
Details: `Ubuntu Update for apache2 USN-1765-1`
OID:1.3.6.1.4.1.25623.1.0.841365
Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2012-3499, CVE-2012-4558, CVE-2012-4557, CVE-2013-1048
Other:
  URL:http://www.ubuntu.com/usn/usn-1765-1/
   USN:1765-1
```

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
postgresql-8.4 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 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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-2483
Other:
  URL:http://www.ubuntu.com/usn/usn-1229-1/
   USN:1229-1
```

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

```
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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-2673
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Other:
  URL:http://www.ubuntu.com/usn/usn-1546-1/
   USN:1546-1
```

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

- 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: `$Revision: 12670 $`

. . . continues on next page . . .

. . . continued from previous page . . .

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-2009-3083, CVE-2009-3084, CVE-2009-3085
BID:36277
Other:
  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
```

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 a 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

. . . continues on next page . . .

. . . continued from previous page . . .

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

Details: `Pidgin OSCAR Protocol Denial Of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800824
Version used: `$Revision: 12670 $`

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
Other:
  URL:http://secunia.com/advisories/35652
   URL:http://developer.pidgin.im/ticket/9483
   URL:http://pidgin.im/pipermail/devel/2009-May/008227.html
```

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

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.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Details: `Ubuntu Update for gnupg USN-1570-1`
OID:1.3.6.1.4.1.25623.1.0.841152
Version used: `$Revision: 14132 $`

References

```
Other:
  URL:http://www.ubuntu.com/usn/usn-1570-1/
   USN:1570-1
```

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`
OID:1.3.6.1.4.1.25623.1.0.841327

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2012-2686, CVE-2013-0166, CVE-2013-0169
Other:
  URL:http://www.ubuntu.com/usn/usn-1732-1/
   USN:1732-1
```

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

Summary

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-3488, CVE-2012-3489
Other:
  URL:http://www.ubuntu.com/usn/usn-1542-1/
   USN:1542-1
```

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.

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 to cause a denial of service. (CVE-2012-0031)
Norman Hippert discovered that the Apache HTTP Server incorrecly 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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-3607, CVE-2011-4317, CVE-2012-0021, CVE-2012-0031, CVE-2012-0053
Other:
  URL:http://www.ubuntu.com/usn/usn-1368-1/
   USN:1368-1
```

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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-4089
Other:
  URL:http://www.ubuntu.com/usn/usn-1308-1/
   USN:1308-1
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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

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: `$Revision: 12629 $`

References

```
CVE: CVE-2009-3274
Other:
  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-Discovere
↪d%29-video.aspx
   URL:http://www.mozilla.com/en-US/firefox/
```

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

```
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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-2143, CVE-2012-2655
Other:
  URL:http://www.ubuntu.com/usn/usn-1461-1/
   USN:1461-1
```

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

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

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Ubuntu Update for apr USN-1134-1`
OID:1.3.6.1.4.1.25623.1.0.840667
Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2011-0419, CVE-2011-1928
Other:
  URL:http://www.ubuntu.com/usn/usn-1134-1/
   USN:1134-1
```

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

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-5668, CVE-2012-5669, CVE-2012-5670
Other:
  URL:http://www.ubuntu.com/usn/usn-1686-1/
   USN:1686-1
```

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
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: `$Revision: 14132 $`

References

```
CVE: CVE-2013-0338
Other:
  URL:http://www.ubuntu.com/usn/usn-1782-1/
   USN:1782-1
```

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

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: `$Revision: 14132 $`

References

```
CVE: CVE-2013-1619
Other:
  URL:http://www.ubuntu.com/usn/usn-1752-1/
   USN:1752-1
```

[return to 10.2.2.100]

2.1.18 Medium 22/tcp

Medium (CVSS: 4.3)

NVT: SSH Weak Encryption Algorithms Supported

Summary

The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result

```
The following weak client-to-server encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
rijndael-cbc@lysator.liu.se
The following weak server-to-client encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Solution

Solution type: Mitigation

Disable the weak encryption algorithms.

Vulnerability Insight

The ‘arcfour‘ cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.

The ‘none‘ algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.

A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method

Check if remote ssh service supports Arcfour, none or CBC ciphers.

Details: `SSH Weak Encryption Algorithms Supported`

OID:1.3.6.1.4.1.25623.1.0.105611

Version used: `$Revision: 13581 $`

References

```
Other:
  URL:https://tools.ietf.org/html/rfc4253#section-6.3
   URL:https://www.kb.cert.org/vuls/id/958563
```

[return to 10.2.2.100]

2.1.19 Medium 25/tcp

Medium (CVSS: 6.8)

NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
Multiple vendors' implementations of 'STARTTLS' are prone to a vulnerability that lets attackers inject arbitrary commands.

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

Impact
An attacker can exploit this issue to execute arbitrary commands in the context of the user running the application. Successful exploits can allow attackers to obtain email usernames and passwords.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
The following vendors are affected:
Ipswitch
Kerio
Postfix
Qmail-TLS
Oracle
SCO Group
spamdyke
ISC

Vulnerability Detection Method
Send a special crafted 'STARTTLS' request and check the response.
Details: `Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection .`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.103935
Version used: `$Revision: 13204 $`

References

```
CVE: CVE-2011-0411, CVE-2011-1430, CVE-2011-1431, CVE-2011-1432, CVE-2011-1506,
↪CVE-2011-1575, CVE-2011-1926, CVE-2011-2165
BID:46767
Other:
  URL:http://www.securityfocus.com/bid/46767
   URL:http://kolab.org/pipermail/kolab-announce/2011/000101.html
   URL:http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424
   URL:http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7
   URL:http://www.kb.cert.org/vuls/id/MAPG-8D9M4P
   URL:http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-
↪notes.txt
   URL:http://www.postfix.org/CVE-2011-0411.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
   URL:http://www.pureftpd.org/project/pure-ftpd/news
   URL:http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNot
↪es_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf
   URL:http://www.spamdyke.org/documentation/Changelog.txt
   URL:http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?inclu
↪de_text=1
   URL:http://www.securityfocus.com/archive/1/516901
   URL:http://support.avaya.com/css/P8/documents/100134676
   URL:http://support.avaya.com/css/P8/documents/100141041
   URL:http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html
   URL:http://inoa.net/qmail-tls/vu555316.patch
   URL:http://www.kb.cert.org/vuls/id/555316
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary
The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result

```
The certificate of the remote service expired on 2010-04-16 14:07:45.
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
subject alternative names (SAN):
None
issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Solution
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `$Revision: 11103 $`

Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests

Summary
The Mailserver on this host answers to VRFY and/or EXPN requests.

Vulnerability Detection Result

```
'VRFY root' produces the following answer: 252 2.0.0 root
```

Solution
Solution type: Workaround
Disable VRFY and/or EXPN on your Mailserver.
For postfix add 'disable_vrfy_command=yes' in 'main.cf'.
For Sendmail add the option 'O PrivacyOptions=goaway'.
It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

Vulnerability Insight
VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

Vulnerability Detection Method
Details: `Check if Mailserver answer to VRFY and EXPN requests`
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: `$Revision: 13470 $`

References

```
Other:
  URL:http://cr.yp.to/smtp/vrfy.html
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Summary
This host is prone to an information disclosure vulnerability.

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

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

Solution

Solution type: Mitigation

Possible Mitigations are:

- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight

The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method

Evaluate previous collected information about this service.

Details: `SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.802087

Version used: `$Revision: 11402 $`

References

```
CVE: CVE-2014-3566
BID:70574
Other:
  URL:https://www.openssl.org/~bodo/ssl-poodle.pdf
   URL:https://www.imperialviolet.org/2014/10/14/poodle.html
   URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
   URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit
↪ing-ssl-30.html
```

Medium (CVSS: 4.3)

NVT: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)

Summary

This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.

Vulnerability Detection Result

```
'DHE_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
```

Impact

Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution

Solution type: VendorFix

- Remove support for 'DHE_EXPORT' cipher suites from the service
- If running OpenSSL updateto version 1.0.2b or 1.0.1n or later.

Affected Software/OS

- Hosts accepting 'DHE_EXPORT' cipher suites
- OpenSSL version before 1.0.2b and 1.0.1n

Vulnerability Insight

Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.

Vulnerability Detection Method

Check previous collected cipher suites saved in the KB.

Details: `SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)`

OID:1.3.6.1.4.1.25623.1.0.805188

Version used: `$Revision: 11872 $`

References

```
CVE: CVE-2015-4000
BID:74733
Other:
  URL:https://weakdh.org
   URL:https://weakdh.org/imperfect-forward-secrecy.pdf
   URL:http://openwall.com/lists/oss-security/2015/05/20/8
   URL:https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained
   URL:https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-change
↪s
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Summary

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and S
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪SLv3 protocols and supports one or more ciphers. Those supported ciphers can b
↪e found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.
↪25623.1.0.802067) NVT.
```

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Solution

Solution type: Mitigation

It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

Vulnerability Insight

The SSLv2 and SSLv3 protocols containing known cryptographic flaws like:
- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)
- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

Vulnerability Detection Method

Check the used protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `$Revision: 5547 $`

References

```
CVE: CVE-2016-0800, CVE-2014-3566
Other:
  URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/delivera
↪bles/algorithms-key-sizes-and-parameters-report
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
   URL:https://drownattack.com/
   URL:https://www.imperialviolet.org/2014/10/14/poodle.html
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

Summary

This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

Vulnerability Detection Result

```
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
```

Impact

Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution

Solution type: VendorFix

- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

Affected Software/OS

- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

Vulnerability Insight

Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

Vulnerability Detection Method

Check previous collected cipher suites saved in the KB.

Details: `SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)`

OID:1.3.6.1.4.1.25623.1.0.805142

Version used: `$Revision: 11872 $`

References

```
CVE: CVE-2015-0204
BID:71936
Other:
  URL:https://freakattack.com
   URL:http://secpod.org/blog/?p=3818
   URL:http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-f
↪actoring-nsa.html
   URL:https://www.openssl.org
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary

The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:                 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173
↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic
↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi
↪ng outside US,C=XX
Signature Algorithm:  sha1WithRSAEncryption
```

Solution

Solution type: Mitigation

Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:

- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:

Fingerprint1

or

fingerprint1,Fingerprint2

Vulnerability Detection Method

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.

Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`

OID:1.3.6.1.4.1.25623.1.0.105880

Version used: `$Revision: 11524 $`

References

```
Other:
  URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪-sha-1-based-signature-algorithms/
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

```
Server Temporary Key Size: 1024 bits
```

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `$Revision: 12865 $`

References

```
Other:
  URL:https://weakdh.org/
   URL:https://weakdh.org/sysadmin.html
```

[return to 10.2.2.100]

2.1.20 Medium 445/tcp

Medium (CVSS: 6.0)
NVT: Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)

Product detection result

```
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

Summary

Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.

Solution

Solution type: VendorFix

Updates are available. Please see the referenced vendor advisory.

Affected Software/OS

This issue affects Samba 3.0.0 to 3.0.25rc3.

Vulnerability Detection Method

Send a crafted command to the samba server and check for a remote command execution.

Details: `Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)`

OID:1.3.6.1.4.1.25623.1.0.108011

Version used: `$Revision: 10398 $`

Product Detection Result

Product: `cpe:/a:samba:samba:3.0.20`

Method: `SMB NativeLanMan`

OID: 1.3.6.1.4.1.25623.1.0.102011)

References

```
CVE: CVE-2007-2447
BID:23972
Other:
  URL:http://www.securityfocus.com/bid/23972
   URL:https://www.samba.org/samba/security/CVE-2007-2447.html
```

[return to 10.2.2.100]

2.1.21 Medium 80/tcp

Medium (CVSS: 6.8)
NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10

Product detection result

```
cpe:/a:twiki:twiki:01.Feb.2003
Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)
```

Summary

The host is running TWiki and is prone to Cross-Site Request Forgery vulnerability.

Vulnerability Detection Result

```
Installed version: 01.Feb.2003
Fixed version:     4.3.2
```

Impact

Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.

Solution

Solution type: VendorFix
Upgrade to TWiki version 4.3.2 or later.

Affected Software/OS

TWiki version prior to 4.3.2

Vulnerability Insight

Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.

Vulnerability Detection Method

Details: `TWiki Cross-Site Request Forgery Vulnerability - Sep10`
OID:1.3.6.1.4.1.25623.1.0.801281
Version used: `$Revision: 12952 $`

Product Detection Result

Product: `cpe:/a:twiki:twiki:01.Feb.2003`
Method: `TWiki Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.800399)

References

```
CVE: CVE-2009-4898
Other:
  URL:http://www.openwall.com/lists/oss-security/2010/08/03/8
   URL:http://www.openwall.com/lists/oss-security/2010/08/02/17
   URL:http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  URL:http://twiki.org/cgi-bin/view/Codev/DownloadTWiki
```

Medium (CVSS: 6.5)
NVT: Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability

Product detection result

```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

Summary

In Tiki the user task component is vulnerable to a SQL Injection via the tiki-user_tasks.php show_history parameter.

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     17.2
```

Solution

Solution type: VendorFix
Upgrade to version 17.2 or later.

Affected Software/OS

Tiki Wiki CMS Groupware prior to version 17.2.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141885
Version used: `$Revision: 13115 $`

Product Detection Result

Product: `cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`
Method: `Tiki Wiki CMS Groupware Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.901001)

References

```
CVE: CVE-2018-20719
Other:
  URL:https://blog.ripstech.com/2018/scan-verify-patch-security-issues-in-minute
↪s/
```

Medium (CVSS: 6.0)
NVT: TWiki Cross-Site Request Forgery Vulnerability

Product detection result

```
cpe:/a:twiki:twiki:01.Feb.2003
Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)
```

Summary

The host is running TWiki and is prone to Cross-Site Request Forgery Vulnerability.

Vulnerability Detection Result

```
Installed version: 01.Feb.2003
Fixed version:     4.3.1
```

Impact

Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.

Solution

Solution type: VendorFix
Upgrade to version 4.3.1 or later.

Affected Software/OS

TWiki version prior to 4.3.1

Vulnerability Insight

Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.

Vulnerability Detection Method

Details: `TWiki Cross-Site Request Forgery Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800400
Version used: `$Revision: 12952 $`

Product Detection Result

Product: `cpe:/a:twiki:twiki:01.Feb.2003`
Method: `TWiki Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.800399)

References

```
CVE: CVE-2009-1339
Other:
  URL:http://secunia.com/advisories/34880
   URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258
   URL:http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-di
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪ff-cve-2009-1339.txt
```

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
Debugging functions are enabled on the remote web server.
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Vulnerability Detection Result

```
The web server has the following HTTP methods enabled: TRACE
```

Impact
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `$Revision: 10828 $`

References

```
CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683,
↪CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, CVE-2012-2223, CVE
↪-2014-7883
BID:9506, 9561, 11604, 15222, 19915, 24456, 33374, 36956, 36990, 37995
Other:
  URL:http://www.kb.cert.org/vuls/id/288308
   URL:http://www.kb.cert.org/vuls/id/867593
   URL:http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
   URL:https://www.owasp.org/index.php/Cross_Site_Tracing
```

Medium (CVSS: 5.0)
NVT: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability

Product detection result

```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

Summary

The host is installed with Tiki Wiki CMS Groupware and is prone to a local file inclusion vulnerability.

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     12.11
```

Impact

Successful exploitation will allow an user having access to the admin backend to gain access to arbitrary files and to compromise the application.

Solution

Solution type: VendorFix
Upgrade to Tiki Wiki CMS Groupware version 12.11 LTS, 15.4 or later.

Affected Software/OS

Tiki Wiki CMS Groupware versions:
- below 12.11 LTS
- 13.x, 14.x and 15.x below 15.4

Vulnerability Insight

The Flaw is due to improper sanitization of input passed to the 'fixedURLData' parameter of the 'display_banner.php' script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.108064
Version used: `2019-05-10T14:24:23+0000`

Product Detection Result

Product: `cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`
Method: `Tiki Wiki CMS Groupware Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.901001)

References

`CVE: CVE-2016-10143`

. . . continues on next page . . .

. . . continued from previous page . . .

```
Other:
  URL:http://tiki.org/article445-Security-updates-Tiki-16-2-15-4-and-Tiki-12-11-
↪released
   URL:https://sourceforge.net/p/tikiwiki/code/60308/
   URL:https://tiki.org
```

Medium (CVSS: 5.0)
NVT: Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability

Product detection result

```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

Summary

The host is installed with Tiki Wiki CMS Groupware and is prone to input sanitation weakness vulnerability.

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     2.2
```

Impact

Successful exploitation could allow arbitrary code execution in the context of an affected site.

Solution

Solution type: VendorFix

Upgrade to version 2.2 or later.

Affected Software/OS

Tiki Wiki CMS Groupware version prior to 2.2 on all running platform

Vulnerability Insight

The vulnerability is due to input validation error in tiki-error.php which fails to sanitise before being returned to the user.

Vulnerability Detection Method

Details: `Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800315
Version used: `$Revision: 14010 $`

Product Detection Result

Product: `cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`
Method: `Tiki Wiki CMS Groupware Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.901001)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
CVE: CVE-2008-5318, CVE-2008-5319
Other:
  URL:http://secunia.com/advisories/32341
    URL:http://info.tikiwiki.org/tiki-read_article.php?articleId=41
```

Medium (CVSS: 5.0)
NVT: /doc directory browsable

Summary

The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.

Vulnerability Detection Result

```
Vulnerable url: http://10.2.2.100/doc/
```

Solution

Solution type: Mitigation

Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:

<Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost </Directory>

Vulnerability Detection Method

Details: `/doc directory browsable`

OID:1.3.6.1.4.1.25623.1.0.10056

Version used: `$Revision: 14336 $`

References

```
CVE: CVE-1999-0678
BID:318
```

Medium (CVSS: 5.0)
NVT: awiki Multiple Local File Include Vulnerabilities

Summary

awiki is prone to multiple local file-include vulnerabilities because it fails to properly sanitize user-supplied input.

Vulnerability Detection Result

```
Vulnerable url: http://10.2.2.100/mutillidae/index.php?page=/etc/passwd
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host. Other attacks are also possible.

Solution

Solution type: WillNotFix

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

Affected Software/OS

awiki 20100125 is vulnerable. Other versions may also be affected.

Vulnerability Detection Method

Details: `awiki Multiple Local File Include Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.103210

Version used: `$Revision: 10741 $`

References

```
BID:49187
Other:
  URL:https://www.exploit-db.com/exploits/36047/
   URL:http://www.securityfocus.com/bid/49187
   URL:http://www.kobaonline.com/awiki/
```

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):
http://10.2.2.100/phpMyAdmin/:pma_password
http://10.2.2.100/phpMyAdmin/?D=A:pma_password
http://10.2.2.100/tikiwiki/tiki-install.php:pass
http://10.2.2.100/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword
```

Impact

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution

Solution type: Workaround

. . . continues on next page . . .

. . . continued from previous page . . .

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.

The script is currently checking the following:

- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'

Details: `Cleartext Transmission of Sensitive Information via HTTP`

OID:1.3.6.1.4.1.25623.1.0.108440

Version used: `$Revision: 10726 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
↪ession_Management
   URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
   URL:https://cwe.mitre.org/data/definitions/319.html
```

Medium (CVSS: 4.3)
NVT: TWiki < 6.1.0 XSS Vulnerability

Product detection result

```
cpe:/a:twiki:twiki:01.Feb.2003
Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)
```

Summary

bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.

Vulnerability Detection Result

```
Installed version: 01.Feb.2003
Fixed version:     6.1.0
```

Solution

Solution type: VendorFix

Update to version 6.1.0 or later.

Affected Software/OS

TWiki version 6.0.2 and probably prior.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `TWiki < 6.1.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141830
Version used: `2019-03-26T08:16:24+0000`

Product Detection Result
Product: `cpe:/a:twiki:twiki:01.Feb.2003`
Method: `TWiki Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.800399)

References

```
CVE: CVE-2018-20212
Other:
  URL:https://seclists.org/fulldisclosure/2019/Jan/7
   URL:http://twiki.org/cgi-bin/view/Codev/DownloadTWiki
```

Medium (CVSS: 4.3)
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

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

Impact
Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

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

Affected Software/OS
phpMyAdmin version 3.3.8.1 and prior.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Vulnerability Detection Method

Details: `phpMyAdmin 'error.php' Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801660
Version used: `$Revision: 11553 $`

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
CVE: CVE-2010-4480
Other:
  URL:http://www.exploit-db.com/exploits/15699/
   URL:http://www.vupen.com/english/advisories/2010/3133
```

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Summary

This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.

Solution

Solution type: VendorFix
Upgrade to Apache HTTP Server version 2.2.22 or later.

Affected Software/OS

Apache HTTP Server versions 2.2.0 through 2.2.21

Vulnerability Insight

The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Details: `Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: `$Revision: 11857 $`

References

```
CVE: CVE-2012-0053
BID:51706
Other:
  URL:http://secunia.com/advisories/47779
   URL:http://www.exploit-db.com/exploits/18442
   URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html
   URL:http://httpd.apache.org/security/vulnerabilities_22.html
   URL:http://svn.apache.org/viewvc?view=revision&revision=1235454
   URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm
↪l
```

[return to 10.2.2.100]

2.1.22 Low general/tcp

Low (CVSS: 3.5)
NVT: Ubuntu Update for net-snmp USN-1450-1

Summary

Ubuntu Update for Linux kernel vulnerabilities USN-1450-1

Vulnerability Detection Result

```
Vulnerable package: libsnmp15
Installed version:  5.4.1~dfsg-4ubuntu4.3
Fixed version:      5.4.1~dfsg-4ubuntu4.4
```

Solution

Solution type: VendorFix
Please Install the Updated Packages.

Affected Software/OS

net-snmp 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 Net-SNMP incorrectly performed entry lookups in the extension table. A remote attacker could send a specially crafted request and cause the SNMP server to crash, leading to a denial of service.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Details: `Ubuntu Update for net-snmp USN-1450-1`
OID:1.3.6.1.4.1.25623.1.0.841015
Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2012-2141
Other:
  URL:http://www.ubuntu.com/usn/usn-1450-1/
   USN:1450-1
```

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: `$Revision: 14132 $`

References

```
CVE: CVE-2009-3297, CVE-2011-0541, CVE-2011-0542, CVE-2011-0543
Other:
  URL:http://www.ubuntu.com/usn/usn-1077-1/
   USN:1077-1
```

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
Version used: `$Revision: 14132 $`

References

```
CVE: CVE-2012-2687, CVE-2012-4929
Other:
  URL:http://www.ubuntu.com/usn/usn-1627-1/
   USN:1627-1
   URL:http://httpd.apache.org/docs/2.4/mod/mod_ssl.html
```

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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-0954
Other:
  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

. . . continues on next page . . .

. . . continued from previous page . . .

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 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: `$Revision: 14132 $`

References

```
CVE: CVE-2012-0954, CVE-2012-3587
Other:
  URL:http://www.ubuntu.com/usn/usn-1475-1/
   USN:1475-1
```

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary

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

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 353095
Packet 2: 353203
```

Impact

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

Solution

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

. . . continues on next page . . .

. . . continued from previous page . . .

See the references for more information.

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

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

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 14310 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
   URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152
```

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: `$Revision: 14132 $`

References

```
CVE: CVE-2011-3634
Other:
  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: `$Revision: 14132 $`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
CVE: CVE-2010-4352
Other:
  URL:http://www.ubuntu.com/usn/usn-1044-1/
   USN:1044-1
```

[return to 10.2.2.100]

2.1.23 Low 22/tcp

Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

Summary
The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Vulnerability Detection Result

```
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
```

Solution
Solution type: Mitigation
Disable the weak MAC algorithms.

Vulnerability Detection Method
Details: `SSH Weak MAC Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `$Revision: 13581 $`

[return to 10.2.2.100]

2.1.24 Low 80/tcp

Low (CVSS: 3.5)
NVT: Tiki Wiki CMS Groupware XSS Vulnerability

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

Summary

An XSS vulnerability (via an SVG image) in Tiki allows an authenticated user to gain administrator privileges if an administrator opens a wiki page with a malicious SVG image, related to lib/filegals/filegallib.php.

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     18.0
```

Solution

Solution type: VendorFix

Upgrade to version 18.0 or later.

Affected Software/OS

Tiki Wiki CMS Groupware prior to version 18.0.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Tiki Wiki CMS Groupware XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.140797

Version used: `$Revision: 12116 $`

Product Detection Result

Product: `cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`

Method: `Tiki Wiki CMS Groupware Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.901001)

References

```
CVE: CVE-2018-7188
Other:
  URL:http://openwall.com/lists/oss-security/2018/02/16/1
```

[return to 10.2.2.100]