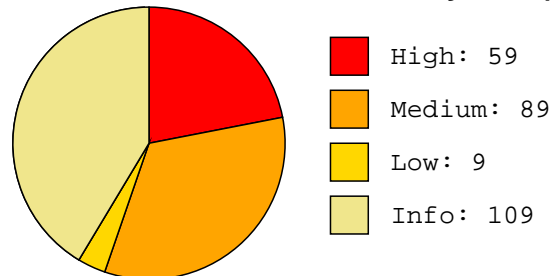




## : I.T Security Vulnerability Report

Job Name:	vulnscan1	Scan time:	2020-04-25 15:25:30
Profile:	Default - Non destructive Full and Fast scan	Generated:	2020-04-25 15:34:11

### Total number of vulnerabilities identified on 1 system(s)



### Total number of vulnerabilities identified per system

HostIP	HostName	Critical	High	Med	Low	Info
192.168.56.12	metasploit	--	59	89	9	109

192.168.56.12

metasploit

High:

Check for Backdoor in UnrealIRCd

Risk: High

Application: irc

Port: 6667

Protocol: tcp

ScriptID: 80111

Solution:

Install latest version of unrealircd

and check signatures of software you're installing.

Insight:

Remote attackers can exploit this issue

to execute arbitrary system commands within the context of the affected application.

The issue affects Unreal 3.2.8.1 for Linux. Reportedly package Unreal3.2.8.1.tar.gz downloaded in November 2009 and later is affected. The MD5 sum of the affected file is 752e46f2d873c1679fa99de3f52a274d. Files with MD5 sum of 7b741e94e867c0a7370553fd01506c66 are not affected.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

Detection of backdoor in UnrealIRCd.

References:

<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

<http://seclists.org/fulldisclosure/2010/Jun/277>

<http://www.securityfocus.com/bid/40820>

CVSS Base Score: 7.5

Family name: Gain a shell remotely

Category: unknown

Copyright: This script is Copyright (C) 2010 Vlatko Kosturjak

Version: \$Revision: 13960 \$

CVEs: CVE-2010-2075

High:

Check for rsh Service

Risk: High

Application: shell

Port: 514

Protocol: tcp

ScriptID: 100080

Vulnerability Detection Result:

The rsh service is misconfigured so it is allowing connections without a password or with default root:root credentials.

Summary:

This remote host is running a rsh service.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

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.

Solution:

Disable the rsh service and use alternatives like SSH instead.

References:

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651>

CVSS Base Score: 7.5

Family name: Useless services

Category: infos

Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 13010 \$

High:

## SSH Brute Force Logins With Default Credentials Reporting

Risk: High

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 103239

Vulnerability Detection Result:

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

msfadmin:msfadmin

postgres:postgres

service:service

user:user

Solution:

Change the password as soon as possible.

Vulnerability Detection Method:

Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials'

(OID: 1.3.6.1.4.1.25623.1.0.108013).

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

It was possible to login into the remote SSH server using default credentials.

As the VT '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 VT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

CVSS Base Score: 7.5

Family name: Default Accounts

Category: end

Copyright: Copyright (c) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-26T13:48:10+0000

High:

Test HTTP dangerous methods

Risk: High

Application: http

Port: 80

Protocol: tcp

ScriptID: 10498

Vulnerability Detection Result:

We could upload the following files via the PUT method at this web server:

<http://192.168.56.12/dav/puttest1557478213.html>

We could delete the following files via the DELETE method at this web server:

<http://192.168.56.12/dav/puttest1557478213.html>

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

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:

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

References:

OWASP:OWASP-CM-001

CVSS Base Score: 7.5

Family name: Remote file access

Category: unknown

Copyright: This script is Copyright (C) 2000 Michel Arboi

Version: 2019-12-04T13:23:25+0000

High:

#### TWiki XSS and Command Execution Vulnerabilities

Risk: High

Application: http

Port: 80

Protocol: tcp

ScriptID: 800320

Vulnerability Detection Result:

Installed version: 01.Feb.2003

Fixed version: 4.2.4

Summary:

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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

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.

Affected Software/OS:

TWiki, TWiki version prior to 4.2.4.

Solution:

Upgrade to version 4.2.4 or later.

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.

References:

<http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304>

<http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5305>

CVSS Base Score: 10.0

Family name: Web application abuses

Category: infos

Copyright: Copyright (C) 2008 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12952 \$

CVEs: CVE-2008-5304, CVE-2008-5305

High:

Ubuntu Update for apache2 USN-1199-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840734

Vulnerability Detection Result:

Vulnerable package: apache2-mpm-prefork

Installed version: 2.2.8-1ubuntu0.15

Fixed version: 2.2.8-1ubuntu0.21

Affected Software/OS:

apache2 on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1199-1

References:

<http://www.ubuntu.com/usn/usn-1199-1/>

USN:1199-1

CVSS Base Score: 7.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-3192

High:

Ubuntu Update for apt USN-1215-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840752

Vulnerability Detection Result:

Vulnerable package: apt

Installed version: 0.7.9ubuntu17

Fixed version: 0.7.9ubuntu17.3

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1215-1

Solution:

Please Install the Updated Packages.

Affected Software/OS:

apt on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

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.

References:

<http://www.ubuntu.com/usn/usn-1215-1/>

USN:1215-1

CVSS Base Score: 10.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$



High:

Ubuntu Update for bind9 USN-1601-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 841182

Vulnerability Detection Result:

Vulnerable package: bind9

Installed version: 9.4.2-10

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

Affected Software/OS:

bind9 on Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 11.04,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1601-1

References:

<http://www.ubuntu.com/usn/usn-1601-1/>

USN:1601-1

CVSS Base Score: 7.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-5166

High:

Ubuntu Update for curl USN-1158-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840685

Vulnerability Detection Result:

Vulnerable package: libcurl3-gnutls

Installed version: 7.18.0-1ubuntu2

Fixed version: 7.18.0-1ubuntu2.3

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1158-1

Solution:

Please Install the Updated Packages.

Affected Software/OS:

curl on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

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.

References:

<http://www.ubuntu.com/usn/usn-1158-1/>

USN:1158-1

CVSS Base Score: 7.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-2192, CVE-2010-0734, CVE-2009-2417

High:

Ubuntu Update for dhcp3 vulnerability USN-1108-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840633

Vulnerability Detection Result:

Vulnerable package: dhcp3-client

Installed version: 3.0.6.dfsg-1ubuntu9

Fixed version: 3.0.6.dfsg-1ubuntu9.2

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1108-1

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.

Solution:

Please Install the Updated Packages.

Affected Software/OS:

dhcp3 vulnerability on Ubuntu 6.06 LTS,

Ubuntu 8.04 LTS,

Ubuntu 9.10,

Ubuntu 10.04 LTS,

Ubuntu 10.10

References:

<http://www.ubuntu.com/usn/usn-1108-1/>

USN:1108-1

CVSS Base Score: 7.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-0997

High:

Ubuntu Update for eglibc USN-1396-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840929

Vulnerability Detection Result:

Vulnerable package: libc6

Installed version: 2.7-10ubuntu5

Fixed version: 2.7-10ubuntu8.1

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1396-1

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

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.

**Solution:**

Please Install the Updated Packages.

**Affected Software/OS:**

eglibc on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

**References:**

<http://www.ubuntu.com/usn/usn-1396-1/>

USN:1396-1

CVSS Base Score: 7.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: 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

High:

Ubuntu Update for eglibc, glibc vulnerability USN-1009-2

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840567

Vulnerability Detection Result:

Vulnerable package: libc6-dev

Installed version: 2.7-10ubuntu5

Fixed version: 2.7-10ubuntu8

Solution:

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

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)

CVSS Base Vector:

AV:L/AC:L/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1009-2

References:

<http://www.ubuntu.com/usn/usn-1009-2/>

USN:1009-2

CVSS Base Score: 7.2

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2010-3847, CVE-2010-3856

High:

Ubuntu Update for freetype USN-1267-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840810

Vulnerability Detection Result:

Vulnerable package: libfreetype6

Installed version: 2.3.5-1ubuntu4.8.04.2

Fixed version: 2.3.5-1ubuntu4.8.04.7

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1267-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:C/I:C/A:C

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)

Affected Software/OS:

freetype on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

References:

<http://www.ubuntu.com/usn/usn-1267-1/>

USN:1267-1

CVSS Base Score: 9.3

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-3256, CVE-2011-3439

High:

Ubuntu Update for freetype USN-1403-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840959

Vulnerability Detection Result:

Vulnerable package: libfreetype6

Installed version: 2.3.5-1ubuntu4.8.04.2

Fixed version: 2.3.5-1ubuntu4.8.04.9

Affected Software/OS:

freetype on Ubuntu 11.10,

Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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)

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1403-1

References:

<http://www.ubuntu.com/usn/usn-1403-1/>

USN:1403-1

CVSS Base Score: 10.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: 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-2012-1141, CVE-2012-1142, CVE-2012-1143, CVE-2012-1144

High:

Ubuntu Update for libpng USN-1367-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840897

Vulnerability Detection Result:

Vulnerable package: libpng12-0

Installed version: 1.2.15~beta5-3ubuntu0.2

Fixed version: 1.2.15~beta5-3ubuntu0.5

Solution:

Please Install the Updated Packages.

Affected Software/OS:

libpng on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

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)

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1367-1

References:

<http://www.ubuntu.com/usn/usn-1367-1/>

USN:1367-1

CVSS Base Score: 7.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2009-5063, CVE-2011-3026

High:

DistCC Remote Code Execution Vulnerability

Risk: High

Application: unknown

Port: 3632

Protocol: tcp

ScriptID: 103553

Vulnerability Detection Result:

It was possible to execute the "id" command.

Result: uid=1(daemon) gid=1(daemon)

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.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:C/I:C/A:C

Impact:

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

Solution:

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

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

References:

<https://distcc.github.io/security.html>

<https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:80/archives/bugtraq/2005-03/0183.html>

CVSS Base Score: 9.3

Family name: General

Category: attack

Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12032 \$

CVEs: CVE-2004-2687

High:

Ubuntu Update for libxml2 USN-1153-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840679

Vulnerability Detection Result:

Vulnerable package: libxml2

Installed version: 2.6.31.dfsg-2ubuntu1

Fixed version: 2.6.31.dfsg-2ubuntu1.6

Affected Software/OS:

libxml2 on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1153-1

References:

<http://www.ubuntu.com/usn/usn-1153-1/>

USN:1153-1

CVSS Base Score: 9.3

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-1944

High:

Ubuntu Update for libxml2 USN-1334-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840868

Vulnerability Detection Result:

Vulnerable package: libxml2

Installed version: 2.6.31.dfsg-2ubuntu1

Fixed version: 2.6.31.dfsg-2ubuntu1.7

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)

Solution:

Please Install the Updated Packages.

Affected Software/OS:

libxml2 on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1334-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:C/I:C/A:C

References:

<http://www.ubuntu.com/usn/usn-1334-1/>

USN:1334-1

CVSS Base Score: 9.3

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-0216, CVE-2011-2821, CVE-2011-2834, CVE-2011-3905, CVE-2011-3919

High:

Ubuntu Update for linux vulnerabilities USN-1072-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840594

Vulnerability Detection Result:

Vulnerable package: linux-libc-dev

Installed version: 2.6.24-27.68

Fixed version: 2.6.24-28.86

CVSS Base Vector:

AV:N/AC:M/Au:S/C:C/I:C/A:N

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1072-1

Insight:

Gleb Napatov discovered that KVM did not correctly check certain privileged operations. A local attacker with access to a guest kernel could exploit this to crash the host system, leading to a denial of service.

(CVE-2010-0435)

Dave Chinner discovered that the XFS filesystem did not correctly order inode lookups when exported by NFS. A remote attacker could exploit this to read or write disk blocks that had changed file assignment or had become unlinked, leading to a loss of privacy. (CVE-2010-2943)

Dan Rosenberg discovered that several network ioctls did not clear kernel memory correctly. A local user could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-3296, CVE-2010-3297)

Dan Jacobson discovered that ThinkPad video output was not correctly access controlled. A local attacker could exploit this to hang the system, leading to a denial of service. (CVE-2010-3448)

It was discovered that KVM did not correctly initialize certain CPU registers. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-3698)

It was discovered that Xen did not correctly clean up threads. A local attacker in a guest system could exploit this to exhaust host system resources, leading to a denial of service. (CVE-2010-3699)

Brad Spengler discovered that stack memory for new a process was not correctly calculated. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-3858)

Dan Rosenberg discovered that the Linux kernel TIPC implementation contained multiple integer signedness errors. A local attacker could exploit this to gain root privileges. (CVE-2010-3859)

Dan Rosenberg discovered that the Linux kernel X.25 implementation incorrectly parsed facilities. A remote attacker could exploit this to crash the kernel, leading to a denial of service. (CVE-2010-3873)

Vasiliy Kulikov discovered that the Linux kernel X.25 implementation did not correctly clear kernel memory. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-3875)

Vasiliy Kulikov discovered that the Linux kernel sockets implementation did not properly initialize certain structures. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy.

(CVE-2010-3876)

Vasiliy Kulikov discovered that the TIPC interface did not correctly initialize certain structures. A local attacker could exploit this to read kernel stack memory, leading to a l ...

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

**Solution:**

Please Install the Updated Packages.

**Affected Software/OS:**

linux vulnerabilities on Ubuntu 8.04 LTS

**References:**

<http://www.ubuntu.com/usn/usn-1072-1/>

USN:1072-1

CVSS Base Score: 7.9

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: 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-2010-4074, CVE-2010-4078, CVE-2010-4079, CVE-2010-4080, CVE-2010-4081, CVE-2010-4083, CVE-2010-4157, CVE-2010-4160, CVE-2010-4248

High:

Ubuntu Update for linux vulnerabilities USN-1105-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840632

Vulnerability Detection Result:

Vulnerable package: linux-libc-dev

Installed version: 2.6.24-27.68

Fixed version: 2.6.24-29.88

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1105-1

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:C

Affected Software/OS:

linux vulnerabilities on Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

Insight:

Dan Rosenberg discovered that multiple terminal ioctls did not correctly initialize structure memory. A local attacker could exploit this to read portions of kernel stack memory, leading to a loss of privacy.

(CVE-2010-4075, CVE-2010-4076, CVE-2010-4077)

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

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

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

Dan Rosenberg discovered multiple flaws in the X.25 facilities parsing.

If a system was using X.25, a remote attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-4164)

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

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

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

References:

<http://www.ubuntu.com/usn/usn-1105-1/>

USN:1105-1



CVSS Base Score: 7.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: 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

High:

## Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities

Risk: High

Application: unknown

Port: 8787

Protocol: tcp

ScriptID: 108010

Vulnerability Detection Result:

The service is running in \$SAFE >= 1 mode. However it is still possible to run arbitrary syscall commands on the remote host. Sending an invalid syscall the service 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 `__send__'"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
`main_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:1430:in `run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in
`start'"//usr/lib/ruby/1.8/drb/drb.rb:1427:in `run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in
`initialize'"//usr/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 implemented
```

Solution:

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

- 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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

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 Method:

Send a crafted command to the service and check for a remote command execution via the instance\_eval or syscall requests.

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.

References:

<https://tools.cisco.com/security/center/viewAlert.x?alertId=22750>

<http://www.securityfocus.com/bid/47071>

[http://blog.recurity-labs.com/archives/2011/05/12/druby\\_for\\_penetration\\_testers/](http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_testers/)

<http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html>

CVSS Base Score: 10.0

Family name: Gain a shell remotely

Category: attack

Copyright: Copyright (c) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12338 \$

High:

Ubuntu Update for mysql-5.1 USN-1397-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840944

Vulnerability Detection Result:

Vulnerable package: mysql-server-5.0

Installed version: 5.0.51a-3ubuntu5

Fixed version: 5.0.95-0ubuntu1

Insight:

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

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

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

Please see the references for more information.

Affected Software/OS:

mysql-5.1 on Ubuntu 11.10,

Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:N/AC:M/Au:S/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1397-1

References:

<http://www.ubuntu.com/usn/usn-1397-1/>

USN:1397-1

<http://dev.mysql.com/doc/refman/5.1/en/news-5-1-x.html>

<http://dev.mysql.com/doc/refman/5.0/en/news-5-0-x.html>

<http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html>

CVSS Base Score: 8.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: 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-2010-3677, 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-2010-3836, CVE-2010-3837, CVE-2010-3838, CVE-2010-3839, CVE-2010-3840, CVE-2011-2262, CVE-2012-0075, CVE-2012-0087, CVE-2012-0101, CV

High:

Ubuntu Update for openssl USN-1357-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840887

Vulnerability Detection Result:

Vulnerable package: openssl

Installed version: 0.9.8g-4ubuntu3

Fixed version: 0.9.8g-4ubuntu3.15

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)

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.

Affected Software/OS:

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

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1357-1

References:

<http://www.ubuntu.com/usn/usn-1357-1/>

USN:1357-1

CVSS Base Score: 9.3

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: 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

High:

Ubuntu Update for pango1.0 vulnerabilities USN-1082-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840602

Vulnerability Detection Result:

Vulnerable package: libpango1.0-0

Installed version: 1.20.5-0ubuntu1.1

Fixed version: 1.20.5-0ubuntu1.2

CVSS Base Vector:

AV:N/AC:H/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1082-1

Insight:

Marc Schoenefeld discovered that Pango incorrectly handled certain Glyph Definition (GDEF) tables. If a user were tricked into displaying text with a specially-crafted font, an attacker could cause Pango to crash, resulting in a denial of service. This issue only affected Ubuntu 8.04 LTS and 9.10. (CVE-2010-0421)

Dan Rosenberg discovered that Pango incorrectly handled certain FT\_Bitmap objects. If a user were tricked into displaying text with a specially-crafted font, an attacker could cause a denial of service or execute arbitrary code with privileges of the user invoking the program. The default compiler options for affected releases should reduce the vulnerability to a denial of service. (CVE-2011-0020)

It was discovered that Pango incorrectly handled certain memory reallocation failures. If a user were tricked into displaying text in a way that would cause a reallocation failure, an attacker could cause a denial of service or execute arbitrary code with privileges of the user invoking the program. This issue only affected Ubuntu 9.10, 10.04 LTS and 10.10. (CVE-2011-0064)

Solution:

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

References:

<http://www.ubuntu.com/usn/usn-1082-1/>

USN:1082-1

CVSS Base Score: 7.6

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2010-0421, CVE-2011-0020, CVE-2011-0064

High:

Ubuntu Update for perl USN-1643-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 841232

Vulnerability Detection Result:

Vulnerable package: perl

Installed version: 5.8.8-12ubuntu0.5

Fixed version: 5.8.8-12ubuntu0.7

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1643-1

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

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)

Affected Software/OS:

perl on Ubuntu 12.10,

Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

References:

<http://www.ubuntu.com/usn/usn-1643-1/>

USN:1643-1

CVSS Base Score: 7.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-2939, CVE-2011-3597, CVE-2012-5195, CVE-2012-5526

High:

Ubuntu Update for perl USN-1770-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 841369

Vulnerability Detection Result:

Vulnerable package: perl

Installed version: 5.8.8-12ubuntu0.5

Fixed version: 5.8.8-12ubuntu0.8

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

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

Solution:

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

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.

References:

<http://www.ubuntu.com/usn/usn-1770-1/>

USN:1770-1

CVSS Base Score: 7.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2013 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2013-1667



High:

Ubuntu Update for php5 USN-1126-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840646

Vulnerability Detection Result:

Vulnerable package: php5-cgi

Installed version: 5.2.4-2ubuntu5.10

Fixed version: 5.2.4-2ubuntu5.15

Insight:

Stephane Chazelas discovered that the /etc/cron.d/php5 cron job for

PHP 5.3.5 allows local users to delete arbitrary files via a symlink

attack on a directory under /var/lib/php5/. (CVE-2011-0441)

Raphael Geisert and Dan Rosenberg discovered that the PEAR installer

allows local users to overwrite arbitrary files via a symlink attack on

the package.xml file, related to the (1) download\_dir, (2) cache\_dir,

(3) tmp\_dir, and (4) pear-build-download directories. (CVE-2011-1072,

CVE-2011-1144)

Ben Schmidt discovered that a use-after-free vulnerability in the PHP

Zend engine could allow an attacker to cause a denial of service (heap

memory corruption) or possibly execute arbitrary code. (CVE-2010-4697)

Martin Barbella discovered a buffer overflow in the PHP GD extension

that allows an attacker to cause a denial of service (application crash)

via a large number of anti-aliasing steps in an argument to the

imagepsthext 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.

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

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1126-1

References:

<http://www.ubuntu.com/usn/usn-1126-1/>

USN:1126-1

CVSS Base Score: 7.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: 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-2011-1468, CVE-2011-1469, CVE-2011-1470,  
CVE-2011-1471

High:

Ubuntu Update for php5 USN-1126-2

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840636

Vulnerability Detection Result:

Vulnerable package: php5-cgi

Installed version: 5.2.4-2ubuntu5.10

Fixed version: 5.2.4-2ubuntu5.17

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

Solution:

Please Install the Updated Packages.

Insight:

USN 1126-1 fixed several vulnerabilities in PHP. The fix for

CVE-2010-4697 introduced an incorrect reference counting regression in the Zend engine that caused the PHP interpreter to segfault. This regression affects Ubuntu 6.06 LTS and Ubuntu 8.04 LTS.

The fixes for CVE-2011-1072 and CVE-2011-1144 introduced a regression in the PEAR installer that prevented it from creating its cache directory and reporting errors correctly.

We apologize for the inconvenience.

Original advisory details:

Stephane Chazelas discovered that the /etc/cron.d/php5 cron job for PHP 5.3.5 allows local users to delete arbitrary files via a symlink attack on a directory under /var/lib/php5/. (CVE-2011-0441)

Raphael Geisert and Dan Rosenberg discovered that the PEAR installer allows local users to overwrite arbitrary files via a symlink attack on the package.xml file, related to the (1) download\_dir, (2) cache\_dir, (3) tmp\_dir, and (4) pear-build-download directories. (CVE-2011-1072, CVE-2011-1144)

Ben Schmidt discovered that a use-after-free vulnerability in the PHP Zend engine could allow an attacker to cause a denial of service (heap memory corruption) or possibly execute arbitrary code. (CVE-2010-4697)

Martin Barbella discovered a buffer overflow in the PHP GD extension that allows an attacker to cause a denial of service (application crash) via a large number of anti-aliasing steps in an argument to the imagepsthext 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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1126-2

References:

<http://www.ubuntu.com/usn/usn-1126-2/>

USN:1126-2

CVSS Base Score: 7.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: 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-2011-1468, CVE-2011-1469, CVE-2011-1470, CVE-2011-1471

High:

Ubuntu Update for php5 USN-1231-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840782

Vulnerability Detection Result:

Vulnerable package: php5-cgi

Installed version: 5.2.4-2ubuntu5.10

Fixed version: 5.2.4-2ubuntu5.18

Affected Software/OS:

php5 on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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)

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1231-1

References:

<http://www.ubuntu.com/usn/usn-1231-1/>

USN:1231-1

CVSS Base Score: 7.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-1938, CVE-2011-2202, CVE-2011-2483, CVE-2011-3182, CVE-2011-3267, CVE-2011-1657, CVE-2010-1914, CVE-2010-2484

High:

Ubuntu Update for php5 USN-1358-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840891

Vulnerability Detection Result:

Vulnerable package: php5-cgi

Installed version: 5.2.4-2ubuntu5.10

Fixed version: 5.2.4-2ubuntu5.22

Insight:

It was discovered that PHP computed hash values for form parameters without restricting the ability to trigger hash collisions predictably.

This could allow a remote attacker to cause a denial of service by sending many crafted parameters. (CVE-2011-4885)

ATTENTION: this update changes previous PHP behavior by limiting the number of external input variables to 1000.

This may be increased by adding a 'max\_input\_vars'

directive to the php.ini configuration file. See

the references for more information.

Stefan Esser discovered that the fix to address the predictable hash collision issue, CVE-2011-4885, did not properly handle the situation where the limit was reached. This could allow a remote attacker to cause a denial of service or execute arbitrary code via a request containing a large number of variables. (CVE-2012-0830)

It was discovered that PHP did not always check the return value of the zend\_strndup function. This could allow a remote attacker to cause a denial of service. (CVE-2011-4153)

It was discovered that PHP did not properly enforce libxslt security settings. This could allow a remote attacker to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension. (CVE-2012-0057)

It was discovered that PHP did not properly enforce that PDORow objects could not be serialized and not be saved in a session. A remote attacker could use this to cause a denial of service via an application crash. (CVE-2012-0788)

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)

Solution:

Please Install the Updated Packages.

Affected Software/OS:

php5 on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1358-1

References:

<http://www.ubuntu.com/usn/usn-1358-1/>

USN:1358-1

<http://www.php.net/manual/en/info.configuration.php#ini.max-input-vars>

CVSS Base Score: 7.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-4885, CVE-2012-0830, CVE-2011-4153, CVE-2012-0057, CVE-2012-0788, CVE-2012-0831, CVE-2011-0441



High:

Ubuntu Update for php5 USN-1358-2

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840895

Vulnerability Detection Result:

Vulnerable package: php5-cgi

Installed version: 5.2.4-2ubuntu5.10

Fixed version: 5.2.4-2ubuntu5.23

Solution:

Please Install the Updated Packages.

Affected Software/OS:

php5 on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Insight:

USN 1358-1 fixed multiple vulnerabilities in PHP. The fix for CVE-2012-0831 introduced a regression where the state of the magic\_quotes\_gpc setting was not correctly reflected when calling the ini\_get() function.

We apologize for the inconvenience.

Original advisory details:

It was discovered that PHP computed hash values for form parameters without restricting the ability to trigger hash collisions predictably.

This could allow a remote attacker to cause a denial of service by sending many crafted parameters. (CVE-2011-4885)

ATTENTION: this update changes previous PHP behavior by limiting the number of external input variables to 1000.

This may be increased by adding a 'max\_input\_vars' directive to the php.ini configuration file. See the references for more information.

Stefan Esser discovered that the fix to address the predictable hash collision issue, CVE-2011-4885, did not properly handle the situation where the limit was reached. This could allow a remote attacker to cause a denial of service or execute arbitrary code via a request containing a large number of variables. (CVE-2012-0830)

It was discovered that PHP did not always check the return value of the zend\_strndup function. This could allow a remote attacker to cause a denial of service. (CVE-2011-4153)

It was discovered that PHP did not properly enforce libxslt security settings. This could allow a remote attacker to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension. (CVE-2012-0057)

It was discovered that PHP did not properly enforce that PDORow objects could not be serialized and not be saved in a session. A remote attacker could use this to cause a denial of service via an application crash. (CVE-2012-0788)

It was discovered that PHP allowed the magic\_quotes\_gpc setting to be disabled remotely. This could allow a remote attacker to bypass

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

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1358-2

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

References:

<http://www.ubuntu.com/usn/usn-1358-2/>

USN:1358-2

<http://www.php.net/manual/en/info.configuration.php#ini.max-input-vars>

CVSS Base Score: 7.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-0831, CVE-2011-4885, CVE-2012-0830, CVE-2011-4153, CVE-2012-0057, CVE-2012-0788,  
CVE-2011-0441

High:

Ubuntu Update for php5 USN-1437-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 841002

Vulnerability Detection Result:

Vulnerable package: php5-cgi

Installed version: 5.2.4-2ubuntu5.10

Fixed version: 5.2.4-2ubuntu5.24

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.

Solution:

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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1437-1

References:

<http://www.ubuntu.com/usn/usn-1437-1/>

USN:1437-1

<http://people.canonical.com/~ubuntu-security/cve/2012/CVE-2012-2311.html>

CVSS Base Score: 7.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-2311, CVE-2012-1823

High:

Ubuntu Update for postgresql-9.1 USN-1789-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 841385

Vulnerability Detection Result:

Vulnerable package: postgresql-8.3

Installed version: 8.3.1-1

Fixed version: 8.3.23-0ubuntu8.04.1

Insight:

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

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

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:N/AC:M/Au:S/C:C/I:C/A:C

Summary:

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

References:

USN:1789-1

<http://www.ubuntu.com/usn/usn-1789-1/>

CVSS Base Score: 8.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2013 Greenbone Networks GmbH

Summary: Check for the Version of postgresql-9.1

Version: \$Revision: 14132 \$

CVEs: CVE-2013-1899, CVE-2013-1900, CVE-2013-1901

High:

Ubuntu Update for samba USN-1374-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840908

Vulnerability Detection Result:

Vulnerable package: samba

Installed version: 3.0.20-0.1ubuntu1

Fixed version: 3.0.28a-1ubuntu4.17

CVSS Base Vector:

AV:A/AC:M/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1374-1

Solution:

Please Install the Updated Packages.

Affected Software/OS:

samba on Ubuntu 8.04 LTS

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.

References:

<http://www.ubuntu.com/usn/usn-1374-1/>

USN:1374-1

CVSS Base Score: 7.9

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-0870

High:

Ubuntu Update for samba USN-1423-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840980

Vulnerability Detection Result:

Vulnerable package: samba

Installed version: 3.0.20-0.1ubuntu1

Fixed version: 3.0.28a-1ubuntu4.18

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1423-1

Solution:

Please Install the Updated Packages.

Affected Software/OS:

samba on Ubuntu 11.10,

Ubuntu 11.04,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

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)

References:

<http://www.ubuntu.com/usn/usn-1423-1/>

USN:1423-1

CVSS Base Score: 10.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-1182

High:

Ubuntu Update for sudo USN-1442-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 841006

Vulnerability Detection Result:

Vulnerable package: sudo

Installed version: 1.6.9p10-1ubuntu3

Fixed version: 1.6.9p10-1ubuntu3.9

Affected Software/OS:

sudo on Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 11.04,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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.

CVSS Base Vector:

AV:L/AC:L/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1442-1

References:

<http://www.ubuntu.com/usn/usn-1442-1/>

USN:1442-1

CVSS Base Score: 7.2

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-2337

High:

Ubuntu Update for tiff regression USN-1085-2

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840613

Vulnerability Detection Result:

Vulnerable package: libtiff4

Installed version: 3.8.2-7ubuntu3.4

Fixed version: 3.8.2-7ubuntu3.8

Affected Software/OS:

tiff regression on Ubuntu 6.06 LTS,

Ubuntu 8.04 LTS,

Ubuntu 9.10,

Ubuntu 10.04 LTS,

Ubuntu 10.10

Solution:

Please Install the Updated Packages.

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 Ghimbovski 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.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1085-2

References:

<http://www.ubuntu.com/usn/usn-1085-2/>

USN:1085-2

CVSS Base Score: 9.3

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

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

High:

Ubuntu Update for tiff USN-1498-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 841073

Vulnerability Detection Result:

Vulnerable package: libtiff4

Installed version: 3.8.2-7ubuntu3.4

Fixed version: 3.8.2-7ubuntu3.12

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1498-1

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Affected Software/OS:

tiff on Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 11.04,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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)

References:

<http://www.ubuntu.com/usn/usn-1498-1/>

USN:1498-1

CVSS Base Score: 7.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-2088, CVE-2012-2113

High:

Ubuntu Update for tiff vulnerabilities USN-1085-1

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 840610

Vulnerability Detection Result:

Vulnerable package: libtiff4

Installed version: 3.8.2-7ubuntu3.4

Fixed version: 3.8.2-7ubuntu3.7

Solution:

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

Insight:

Sauli Pahlman discovered that the TIFF library incorrectly handled invalid `td_stripbytecount` fields. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2010-2482)

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

Nicolae Ghimbovski 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)

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1085-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:C/I:C/A:C

References:

<http://www.ubuntu.com/usn/usn-1085-1/>

USN:1085-1

CVSS Base Score: 9.3

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: 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

High:

VNC Brute Force Login

Risk: High

Application: vnc

Port: 5900

Protocol: tcp

ScriptID: 106056

Vulnerability Detection Result:

It was possible to connect to the VNC server with the password: password

Insight:

This script tries to authenticate to a VNC server with

the passwords set in the password preference. It will also test and report if no authentication / password is required at all.

Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked.

Note as well that passwords can be max. 8 characters long.

Solution:

Change the password to something hard to guess or enable password protection at all.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:P/A:P

Summary:

Try to log in with given passwords via VNC protocol.

CVSS Base Score: 9.0

Family name: Brute force attacks

Category: attack

Copyright: This script is Copyright (C) 2015 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-12-03T12:31:12+0000

High:

#### FTP Brute Force Logins Reporting

Risk: High

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 108718

#### Vulnerability Detection Result:

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

msfadmin:msfadmin

postgres:postgres

service:service

user:user

#### Summary:

It was possible to login into the remote FTP server using weak/known credentials.

As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

#### CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

#### Vulnerability Detection Method:

Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).

#### Solution:

Change the password as soon as possible.

CVSS Base Score: 7.5

Family name: Brute force attacks

Category: unknown

Copyright: Copyright (C) 2020 Greenbone Networks GmbH

Version: 2020-03-24T12:27:11+0000

High:

vsftpd Compromised Source Packages Backdoor Vulnerability

Risk: High

Application: unknown

Port: 6200

Protocol: tcp

ScriptID: 103185

Impact:

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

Summary:

vsftpd is prone to a backdoor vulnerability.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Affected Software/OS:

The vsftpd 2.3.4 source package is affected.

Solution:

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

References:

<http://www.securityfocus.com/bid/48539>

<http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html>

<https://security.appspot.com/vsftpd.html>

CVSS Base Score: 7.5

Family name: Gain a shell remotely

Category: attack

Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12076 \$

High:

vsftpd Compromised Source Packages Backdoor Vulnerability

Risk: High

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 103185

Solution:

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

vsftpd is prone to a backdoor vulnerability.

Impact:

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

References:

<http://www.securityfocus.com/bid/48539>

<http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html>

<https://security.appspot.com/vsftpd.html>

CVSS Base Score: 7.5

Family name: Gain a shell remotely

Category: attack

Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12076 \$



High:

## GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC)

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 804490

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

Solution:

Apply the patch or upgrade to latest version.

Affected Software/OS:

GNU Bash through 4.3

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.

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.

Vulnerability Detection Method:

Login to the target machine with ssh

credentials and check its possible to execute the commands via GNU bash shell.

Summary:

This host is installed with GNU Bash Shell

and is prone to remote command execution vulnerability.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

References:

<https://access.redhat.com/solutions/1207723>

[https://bugzilla.redhat.com/show\\_bug.cgi?id=1141597](https://bugzilla.redhat.com/show_bug.cgi?id=1141597)

<https://blogs.akamai.com/2014/09/environment-bashing.html>

<https://community.qualys.com/blogs/securitylabs/2014/09/24/>

<http://www.gnu.org/software/bash/>

CVSS Base Score: 10.0

Family name: General

Category: attack

Copyright: Copyright (C) 2014 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12551 \$

CVEs: CVE-2014-6271

High:

## GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 02

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 802082

Vulnerability Detection Result:

Used command: echo "cd /tmp; rm -f /tmp/echo; env X='() { (VT Test)=>' /bin/bash -c 'echo id'; cat echo; rm -f /tmp/echo" | /bin/bash

Result: /bin/bash: X: line 1: syntax error near unexpected token `='

/bin/bash: X: line 1: ``

/bin/bash: error importing function definition for `X'

uid=1000(msfadmin) gid=1000(msfadmin)

groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)

Affected Software/OS:

GNU Bash through 4.3 bash43-025

Solution:

Apply the patch from the referenced advisory.

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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

Summary:

This host is installed with GNU Bash Shell

and is prone to remote command execution vulnerability.

Vulnerability Detection Method:

Login to the target machine with ssh

credentials and check its possible to execute the commands via GNU bash shell.

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.

References:

<https://ftp.gnu.org/gnu/bash/>

<https://shellshocker.net/>

<http://www.kb.cert.org/vuls/id/252743>

<http://www.openwall.com/lists/oss-security/2014/09/24/32>

<https://community.qualys.com/blogs/securitylabs/2014/09/24/bash-remote-code-execution-vulnerability-cve-2014-6271>

1

CVSS Base Score: 10.0

Family name: General

Category: attack

Copyright: Copyright (C) 2014 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12551 \$

CVEs: CVE-2014-7169

High:

## GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 03

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 802085

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

Vulnerability Detection Method:

Login to the target machine with ssh

credentials and check its possible to execute the commands via GNU bash shell.

Summary:

This host is installed with GNU Bash Shell

and is prone to remote command execution vulnerability.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

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.

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

Solution:

Apply the patch from the referenced advisory.

Affected Software/OS:

GNU Bash through 4.3 bash43-026

References:

<https://ftp.gnu.org/gnu/bash/>

<https://shellshocker.net/>

<http://lcamtuf.blogspot.in/2014/09/bash-bug-apply-unofficial-patch-now.html>

CVSS Base Score: 10.0

Family name: General

Category: attack

Copyright: Copyright (C) 2014 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12551 \$

CVEs: CVE-2014-6278

High:

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

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 802086

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: 16955 Segmentation fault vt\_test=()' { x() { \_;}; x() { \_;} <<a; }' /bin/bash -c date 2>/dev/null

CVE-2014-6277 vulnerable

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

Affected Software/OS:

GNU Bash through 4.3 bash43-026

Solution:

Apply the patch from the referenced advisory.

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

Summary:

This host is installed with GNU Bash Shell

and is prone to remote command execution vulnerability.

Vulnerability Detection Method:

Login to the target machine with ssh

credentials and check its possible to execute the commands via GNU bash shell.

References:

<https://shellshocker.net>

<http://lcamtuf.blogspot.in/2014/09/bash-bug-apply-unofficial-patch-now.html>

<https://ftp.gnu.org/gnu/bash/>

CVSS Base Score: 10.0

Family name: General

Category: attack

Copyright: Copyright (C) 2014 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12551 \$

CVEs: CVE-2014-6277

High:

## GNU Bash Stacked Redirects aka 'redir\_stack' Memory Corruption Vulnerability (LSC)

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 802083

### 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: 24542 Segmentation fault    /bin/bash -c 'true <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF  
<<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF'
```

CVE-2014-7186 vulnerable, redir\_stack

Summary:

This host is installed with GNU Bash Shell

and is prone to command execution vulnerability.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

## Vulnerability Detection Method:

Login to the target machine with ssh

credentials and check its possible to execute the commands via GNU bash shell.

Impact:

Successful exploitation will allow

attackers to corrupt memory to cause a crash or potentially execute arbitrary coommands.

Insight:

GNU bash contains a flaw that is triggered

when evaluating untrusted input during stacked redirects handling.

Affected Software/OS:

## GNU Bash through 4.3 bash43-026

**Solution:**

Apply the appropriate patch.

References:

<https://shellshocker.net/>

<http://openwall.com/lists/oss-security/2014/09/26/2>

<http://openwall.com/lists/oss-security/2014/09/25/32>

<http://lcamtuf.blogspot.in/2014/09/bash-bug-apply-unofficial-patch-now.html>

<http://www.gnu.org/software/bash/>

CVSS Base Score: 10.0

Family name: General

Category: attack

Copyright: Copyright (C) 2014 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12551 \$

CVEs: CVE-2014-7186

High:

# Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability

Risk: High

Application: unknown

Port: 1099

Protocol: tcp

ScriptID: 140051

Solution:

Disable class-loading.

Insight:

The vulnerability exists because of an incorrect default configuration of the Remote Method Invocation (RMI) Server in the affected software.

Vulnerability Detection Method:

Check if the target tries to load a Java class via a remote HTTP URL.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

Summary:

Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.

Impact:

An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted packets to the affected software. When the packets are processed, the attacker could execute arbitrary code on the system with elevated privileges.

References:

<https://tools.cisco.com/security/center/viewAlert.x?alertId=23665>

CVSS Base Score: 10.0

Family name: General

Category: attack

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 13999 \$

High:

MySQL / MariaDB weak password

Risk: High

Application: mysql

Port: 3306

Protocol: tcp

ScriptID: 103551

Vulnerability Detection Result:

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

Solution:

Change the password as soon as possible.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:P/A:P

Summary:

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

CVSS Base Score: 9.0

Family name: Default Accounts

Category: attack

Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-09-06T14:17:49+0000

High:

OS End Of Life Detection

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 103674

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>

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

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.

Solution:

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

CVSS Base Score: 10.0

Family name: General

Category: infos

Copyright: This script is Copyright (C) 2013 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-10-21T09:55:06+0000

High:

### Apache Tomcat AJP RCE Vulnerability

Risk: High

Application: ajp13

Port: 8009

Protocol: tcp

ScriptID: 143545

Vulnerability Detection Result:

It was possible to read the file "/WEB-INF/web.xml" through the ajp13 connector.

Result:

AB 8 Ã^ OK Content-Type text/html; charset=ISO-8859-1 AB Ã¼ Ã\_<!--

Licensed to the Apache Software Foundation (ASF) under one or more contributor license agreements. See the NOTICE file distributed with this work for additional information regarding copyright ownership.

The ASF licenses this file to You under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

-->

<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"

"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

<head>

<title>Apache Tomcat/5.5</title>

<style type="text/css">

/\*<![CDATA[\*/

body {

color: #000000;

background-color: #FFFFFF;

font-family: Arial, "Times New Roman", Times, serif;

margin: 10px 0px;

}

img {

border: none;

}

a:link, a:visited {

color: blue

}

th {

font-family: Verdana, "Times New Roman", Times, serif;

font-size: 110%;

font-weight: normal;

font-style: italic;

background: #D2A41C;

text-align: left;



```

}
td {
    color: #000000;
font-family: Arial, Helvetica, sans-serif;
}

td.menu {
    background: #FFDC75;
}
.center {
    text-align: center;
}
.code {
    color: #000000;
    font-family: "Courier New", Courier, monospace;
    font-size: 110%;
    margin-left: 2.5em;
}

#banner {
    margin-bottom: 12px;
}
p#congrats {
    margin-top: 0;
    font-weight: bold;
    text-align: center;
}
p#footer {
    text-align: right;
    font-size: 80%;
}
/*]]>*/
</style>
</head>
<body>
<!-- Header -->
<table id="banner" width="100%">
    <tr>
        <td align="left" style="width:130px">
            <a href="http://tomcat.apache.org/">
                
            </a>
        </td>
        <td align="left" valign="top"><b>Apache Tomcat/5.5</b></td>
        <td align="right">
            <a href="http://www.apache.org/">
                
            </a>
        </td>
    </tr>
</table>
<table>
    <tr>

```

```

<!-- Table of Contents -->
<td valign="top">
  <table width="100%" border="1" cellspacing="0" cellpadding="3">
    <tr>
<th>Administration</th>
    </tr>
    <tr>
<td class="menu">
    <a href="manager/status">Status</a><br/>
      <a href="admin">TomcatÂ Administration</a><br/>
      <a href="manager/html">TomcatÂ Manager</a><br/>
      Â
    </td>
    </tr>
  </table>
<br />
  <table width="100%" border="1" cellspacing="0" cellpadding="3">
    <tr>
<th>Documentation</th>
    </tr>
    <tr>
      <td class="menu">
        <a href="RELEASE-NOTES.txt">ReleaseÂ Notes</a><br/>
        <a href="tomcat-docs/changelog.html">ChangeÂ Log</a><br/>
        <a href="tomcat-docs">TomcatÂ Documentation</a><br/>
        Â
      </td>
      <td>Â
    </tr>
  </table>

<br/>
  <table width="100%" border="1" cellspacing="0" cellpadding="3">
    <tr>
      <th>Tomcat Online</th>
    </tr>
    <tr>
      <td class="menu">
        <a href="http://tomcat.apache.org/">HomeÂ Page</a><br/>
<a href="http://tomcat.apache.org/faq/">FAQ</a><br/>
        <a href="http://tomcat.apache.org/bugreport.html">BugÂ Database</a><br/>
        <a
href="http://issues.apache.org/bugzilla/buglist.cgi?bug_status=UNCONFIRMED&bug_status=NEW&bug_status=ASSIG
NED&bug_status=REOPENED&bug_status=RESOLVED&resolution=LATER&resolution=REMIND&resolution=---&bugi
dtype=include&product=Tomcat+5&cmdtype=doit&order=Importance">Open Bugs</a><br/>
        <a href="http://mail-archives.apache.org/mod_mbox/tomcat-users/">UsersÂ MailingÂ List</a><br/>
        <a href="http://mail-archives.apache.org/mod_mbox/tomcat-dev/">DevelopersÂ MailingÂ List</a><br/>
        <a href="irc://irc.freenode.net/#tomcat">IRC</a><br/>
        Â
      </td>
    </tr>
  </table>

<br/>

```

```

<table width="100%" border="1" cellspacing="0" cellpadding="3">
  <tr>
    <th>Examples</th>
  </tr>
  <tr>
    <td class="menu">
      <a href="jsp-examples/">JSPÂ Examples</a><br/>
      <a href="servlets-examples/">ServletÂ Examples</a><br/>
      <a href="webdav/">WebDAVÂ capabilities</a><br/>
    </td>
  </tr>
</table>

```

```

<br/>
<table width="100%" border="1" cellspacing="0" cellpadding="3">
  <tr>
    <th>Miscellaneous</th>
  </tr>
  <tr>
    <td class="menu">
      <a href="http://java.sun.com/products/jsp">Sun'sÂ JavaÂ ServerÂ PagesÂ Site</a><br/>
      <a href="http://java.sun.com/products/servlet">Sun'sÂ ServletÂ Site</a><br/>
    </td>
  </tr>
</table>

```

```

</td>
<td style="width:20px">Â </td>

```

```

<!-- Body -->

```

```

<td align="left" valign="top">

```

```

  <p id="congrats">If you're seeing this page via a web browser, it means you've setup Tomcat successfully.
  Congratulations!</p>

```

```

  <p>As you may have guessed by now, this is the default Tomcat home page. It can be found on the local
  filesystem at:</p>

```

```

  <p class="code">${CATALINA_HOME}/webapps/ROOT/index.jsp</p>

```

```

  <p>where "${CATALINA_HOME}" is the root of the Tomcat installation directory. If you're seeing this page, and
  you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an
  administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the <a
  href="tomcat-docs">Tomcat Documentation</a> for more detailed setup and administration information than is found in
  the INSTALL file.</p>

```

```

  <p><b>NOTE:</b> This page is precompiled. If you change it, this page will not change since
  it was compiled into a servlet at build time.

```

```

  (See <tt>${CATALINA_HOME}/webapps/ROOT/WEB-INF/web.xml</tt> as to how it was mapped.)

```

```

</p>

```

```

<p><b>NOTE: For security reasons, using the administration webapp
is restricted to users with role "admin". The manager webapp
is restricted to users with role "manager".</b>

```

```

Users are defined in <code>${CATALINA_HOME}/conf/tomcat-users.xml</code>.</p>

```

```

<p>Included with this release are a host of sample Servlets and JSPs (with associated source code),

```

extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

[users@tomc](mailto:users@tomcat.apache.org)

Vulnerability Detection Method:

Sends a crafted AJP13 request and checks the response.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

Apache Tomcat is prone to a remote code execution vulnerability in the AJP connector dubbed 'Ghostcat'.

Solution:

Update to version 7.0.100, 8.5.51, 9.0.31 or later.

Affected Software/OS:

Apache Tomcat versions prior 7.0.100, 8.5.51 or 9.0.31 when the AJP connector is enabled.

Insight:

Apache Tomcat server has a file containing vulnerability, which can be used by an attacker to read or include any files in all webapp directories on Tomcat, such as webapp configuration files or source code.

References:

<https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E>

<https://www.chaitin.cn/en/ghostcat>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487>

<https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi>

<https://tomcat.apache.org/tomcat-7.0-doc/changelog.html>

<https://tomcat.apache.org/tomcat-8.5-doc/changelog.html>

<https://tomcat.apache.org/tomcat-9.0-doc/changelog.html>

CVSS Base Score: 7.5

Family name: Web application abuses

Category: unknown

Copyright: Copyright (C) 2020 Greenbone Networks GmbH

Version: 2020-03-25T03:34:54+0000

CVEs: CVE-2020-1938

High:

PHP-CGI-based setups vulnerability when parsing query string parameters from php files.

Risk: High

Application: http

Port: 80

Protocol: tcp

ScriptID: 103482

Vulnerability Detection Result:

Vulnerable url: <http://192.168.56.12/cgi-bin/php>

Solution:

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.

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>

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

PHP is prone to an information-disclosure vulnerability.

References:

<http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-risks-Update-1567532.html>

<http://www.kb.cert.org/vuls/id/520827>

<http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/>

<https://bugs.php.net/bug.php?id=61910>

<http://www.php.net/manual/en/security.cgi-bin.php>

<http://www.securityfocus.com/bid/53388>

CVSS Base Score: 7.5

Family name: Web application abuses

Category: attack

Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-11-08T10:10:55+0000

CVEs: CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335

High:

phpinfo() output Reporting

Risk: High

Application: http

Port: 80

Protocol: tcp

ScriptID: 11229

Vulnerability Detection Result:

The following files are calling the function phpinfo() which disclose potentially sensitive information:

<http://192.168.56.12/mutillidae/phpinfo.php>

<http://192.168.56.12/phpinfo.php>

Solution:

Delete the listed files or restrict access to them.

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.

Summary:

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS Base Score: 7.5

Family name: Web application abuses

Category: unknown

Copyright: This script is Copyright (C) 2003 Randy Matz

Version: \$Revision: 11992 \$

High:

Pidgin MSN SLP Packets Denial Of Service Vulnerability (Linux)

Risk: High

Application: general

Port: 0

Protocol: tcp

ScriptID: 900920

Vulnerability Detection Result:

Installed version: 2.5.2

Fixed version: 2.5.9

Summary:

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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

Impact:

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

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.

Solution:

Upgrade to Pidgin version 2.5.9.

Affected Software/OS:

Pidgin version prior to 2.5.9 on Linux.

References:

<http://secunia.com/advisories/36384>

<http://www.pidgin.im/news/security/?id=34>

<http://www.vupen.com/english/advisories/2009/2303>

CVSS Base Score: 10.0

Family name: Denial of Service

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: \$Revision: 12670 \$

CVEs: CVE-2009-2694

High:

Possible Backdoor: Ingreslock

Risk: High

Application: ingreslock

Port: 1524

Protocol: tcp

ScriptID: 103549

Vulnerability Detection Result:

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

Summary:

A backdoor is installed on the remote host.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

Impact:

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

Solution:

A whole cleanup of the infected system is recommended.

CVSS Base Score: 10.0

Family name: Gain a shell remotely

Category: attack

Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-21T13:23:23+0000

High:

PostgreSQL weak password

Risk: High

Application: postgres

Port: 5432

Protocol: tcp

ScriptID: 103552

Vulnerability Detection Result:

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

Solution:

Change the password as soon as possible.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:P/A:P

Summary:

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

CVSS Base Score: 9.0

Family name: Default Accounts

Category: attack

Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-01-28T13:26:39+0000



High:

Check for rexecd Service

Risk: High

Application: exec

Port: 512

Protocol: tcp

ScriptID: 100111

Vulnerability Detection Result:

The rexec service is not allowing connections from this host.

Summary:

This remote host is running a rexec service.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:

Disable the rexec service and use alternatives like SSH instead.

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 authenticates by reading the username and password \*unencrypted\* from the socket.

References:

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0618>

CVSS Base Score: 10.0

Family name: Useless services

Category: infos

Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 13541 \$

High:

Check for rlogin Service

Risk: High

Application: login

Port: 513

Protocol: tcp

ScriptID: 901202

Vulnerability Detection Result:

The service is misconfigured so it is allowing connections without a password.

Solution:

Disable the rlogin service and use alternatives like SSH instead.

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)

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:

This remote host is running a rlogin service.

References:

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651>

<http://en.wikipedia.org/wiki/Rlogin>

<http://www.ietf.org/rfc/rfc1282.txt>

CVSS Base Score: 7.5

Family name: Useless services

Category: infos

Copyright: Copyright (C) 2011 SecPod

Summary: NOSUMMARY

Version: \$Revision: 13541 \$

Medium:

/doc directory browsable

Risk: Medium

Application: http

Port: 80

Protocol: tcp

ScriptID: 10056

Vulnerability Detection Result:

Vulnerable url: http://192.168.56.12/doc/

Solution:

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>
```

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:N/A:N

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.

CVSS Base Score: 5.0

Family name: Web application abuses

Category: unknown

Copyright: This script is Copyright (C) 2000 Hendrik Scholz

Version: 2019-11-22T13:51:04+0000

CVEs: CVE-1999-0678

Medium:

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

Risk: Medium

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 108011

Summary:

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

CVSS Base Vector:

AV:N/AC:M/Au:S/C:P/I:P/A:P

Vulnerability Detection Method:

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

Impact:

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

Affected Software/OS:

This issue affects Samba 3.0.0 to 3.0.25rc3.

Solution:

Updates are available. Please see the referenced vendor advisory.

References:

<http://www.securityfocus.com/bid/23972>

<https://www.samba.org/samba/security/CVE-2007-2447.html>

CVSS Base Score: 6.0

Family name: Gain a shell remotely

Category: attack

Copyright: Copyright (c) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 10398 \$

CVEs: CVE-2007-2447

Medium:

SSL/TLS: Report Weak Cipher Suites

Risk: Medium

Application: postgres

Port: 5432

Protocol: tcp

ScriptID: 103440

Vulnerability Detection Result:

Weak ciphers offered by this service:

SSL3\_RSA\_RC4\_128\_SHA

SSL3\_EDH\_RSA\_DES\_192\_CBC3\_SHA

SSL3\_RSA\_DES\_192\_CBC3\_SHA

TLS1\_RSA\_RC4\_128\_SHA

TLS1\_EDH\_RSA\_DES\_192\_CBC3\_SHA

TLS1\_RSA\_DES\_192\_CBC3\_SHA

Summary:

This routine search for weak SSL ciphers offered by a service.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:N/A:N

Solution:

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Insight:

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

- Any SSL/TLS using no cipher is considered weak.
- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol.
- RC4 is considered to be weak.
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak.
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

CVSS Base Score: 4.3

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 11135 \$

CVEs: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000

Medium:

SSL/TLS: Report Weak Cipher Suites

Risk: Medium

Application: smtp

Port: 25

Protocol: tcp

ScriptID: 103440

Vulnerability Detection Result:

Weak ciphers offered by this service:

SSL2\_RC4\_128\_MD5  
SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5  
SSL2\_DES\_64\_CBC\_WITH\_MD5  
SSL2\_RC2\_CBC\_128\_CBC\_EXPORT40\_WITH\_MD5  
SSL2\_RC2\_CBC\_128\_CBC\_WITH\_MD5  
SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5  
SSL3\_ADH\_RC4\_128\_MD5  
SSL3\_RSA\_RC4\_128\_MD5  
SSL3\_RSA\_RC4\_128\_SHA  
SSL3\_ADH\_RC4\_40\_MD5  
SSL3\_RSA\_RC2\_40\_MD5  
SSL3\_RSA\_RC4\_40\_MD5  
SSL3\_EDH\_RSA\_DES\_192\_CBC3\_SHA  
SSL3\_RSA\_DES\_192\_CBC3\_SHA  
SSL3\_ADH\_DES\_192\_CBC\_SHA  
SSL3\_ADH\_DES\_64\_CBC\_SHA  
SSL3\_ADH\_DES\_40\_CBC\_SHA  
SSL3\_EDH\_RSA\_DES\_64\_CBC\_SHA  
SSL3\_EDH\_RSA\_DES\_40\_CBC\_SHA  
SSL3\_RSA\_DES\_64\_CBC\_SHA  
SSL3\_RSA\_DES\_40\_CBC\_SHA  
TLS1\_ADH\_RC4\_128\_MD5  
TLS1\_RSA\_RC4\_128\_MD5  
TLS1\_RSA\_RC4\_128\_SHA  
TLS1\_ADH\_RC4\_40\_MD5  
TLS1\_RSA\_RC2\_40\_MD5  
TLS1\_RSA\_RC4\_40\_MD5  
TLS1\_EDH\_RSA\_DES\_192\_CBC3\_SHA  
TLS1\_RSA\_DES\_192\_CBC3\_SHA  
TLS1\_ADH\_DES\_192\_CBC\_SHA  
TLS1\_ADH\_DES\_64\_CBC\_SHA  
TLS1\_ADH\_DES\_40\_CBC\_SHA  
TLS1\_EDH\_RSA\_DES\_64\_CBC\_SHA  
TLS1\_EDH\_RSA\_DES\_40\_CBC\_SHA  
TLS1\_RSA\_DES\_64\_CBC\_SHA  
TLS1\_RSA\_DES\_40\_CBC\_SHA

Summary:

This routine search for weak SSL ciphers offered by a service.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:N/A:N

Insight:

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

- Any SSL/TLS using no cipher is considered weak.

- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol.
- RC4 is considered to be weak.
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak.
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Solution:

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

CVSS Base Score: 4.3

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 11135 \$

CVEs: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000

Medium:

Check if Mailserver answer to VRFY and EXPN requests

Risk: Medium

Application: smtp

Port: 25

Protocol: tcp

ScriptID: 100072

Vulnerability Detection Result:

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

Solution:

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.

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.

Summary:

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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

<http://cr.yp.to/smtp/vrfy.html>

CVSS Base Score: 5.0

Family name: SMTP problems

Category: infos

Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-23T13:51:29+0000



Medium:

### SSH Weak Encryption Algorithms Supported

Risk: Medium

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 105611

Vulnerability Detection Result:

The following weak client-to-server encryption algorithms are supported by the remote service:

3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc

arcfour

arcfour128

arcfour256

blowfish-cbc

cast128-cbc

rijndael-cbc@lysator.liu.se

The following weak server-to-client encryption algorithms are supported by the remote service:

3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc

arcfour

arcfour128

arcfour256

blowfish-cbc

cast128-cbc

rijndael-cbc@lysator.liu.se

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.

Solution:

Disable the weak encryption algorithms.

Vulnerability Detection Method:

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

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:N/A:N

Summary:

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

References:

<https://tools.ietf.org/html/rfc4253#section-6.3>

<https://www.kb.cert.org/vuls/id/958563>

CVSS Base Score: 4.3

Family name: General

Category: infos

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-26T13:48:10+0000

Medium:

SSL/TLS: Certificate Expired

Risk: Medium

Application: smtp

Port: 25

Protocol: tcp

ScriptID: 103955

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=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX

subject alternative names (SAN):

None

issued by .:

1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside 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): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436DE813CC

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:P/A:N

Summary:

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

Insight:

This script checks expiry dates of certificates associated with

SSL/TLS-enabled services on the target and reports whether any have already expired.

Solution:

Replace the SSL/TLS certificate by a new one.

CVSS Base Score: 5.0

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2013 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 11103 \$

Medium:

SSL/TLS: Certificate Expired

Risk: Medium

Application: postgres

Port: 5432

Protocol: tcp

ScriptID: 103955

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=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX

subject alternative names (SAN):

None

issued by .:

1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside 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): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436DE813CC

Summary:

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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:P/A:N

Solution:

Replace the SSL/TLS certificate by a new one.

Insight:

This script checks expiry dates of certificates associated with

SSL/TLS-enabled services on the target and reports whether any have already expired.

CVSS Base Score: 5.0

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2013 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 11103 \$

Medium:

SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Risk: Medium

Application: postgres

Port: 5432

Protocol: tcp

ScriptID: 105880

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=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX

Signature Algorithm: sha1WithRSAEncryption

Solution:

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.

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

CVSS Base Vector:

AV:N/AC:H/Au:N/C:P/I:P/A:N

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 Method:

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

References:

<https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/>

CVSS Base Score: 4.0

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 11524 \$

Medium:

Cleartext Transmission of Sensitive Information via HTTP

Risk: Medium

Application: http

Port: 80

Protocol: tcp

ScriptID: 108440

Vulnerability Detection Result:

The following input fields were identified (URL:input name):

[http://192.168.56.12/phpMyAdmin/:pma\\_password](http://192.168.56.12/phpMyAdmin/:pma_password)

[http://192.168.56.12/phpMyAdmin/?D=A:pma\\_password](http://192.168.56.12/phpMyAdmin/?D=A:pma_password)

<http://192.168.56.12/tikiwiki/tiki-install.php:pass>

<http://192.168.56.12/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.

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'

CVSS Base Vector:

AV:A/AC:L/Au:N/C:P/I:P/A:N

Summary:

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

Solution:

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.

References:

[https://www.owasp.org/index.php/Top\\_10\\_2013-A2-Broken\\_Authentication\\_and\\_Session\\_Management](https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management)

[https://www.owasp.org/index.php/Top\\_10\\_2013-A6-Sensitive\\_Data\\_Exposure](https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure)

<https://cwe.mitre.org/data/definitions/319.html>

CVSS Base Score: 4.8

Family name: Web application abuses

Category: infos

Copyright: Copyright (C) 2018 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 10726 \$

Medium:

SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Risk: Medium

Application: smtp

Port: 25

Protocol: tcp

ScriptID: 105880

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=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX

Signature Algorithm: sha1WithRSAEncryption

Solution:

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.

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.

Summary:

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

CVSS Base Vector:

AV:N/AC:H/Au:N/C:P/I:P/A:N

References:

<https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/>

CVSS Base Score: 4.0

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 11524 \$

Medium:

SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Risk: Medium

Application: postgres

Port: 5432

Protocol: tcp

ScriptID: 111012

Vulnerability Detection Result:

In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) NVT.

Summary:

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

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:N/A:N

Vulnerability Detection Method:

Check the used protocols of the services provided by this system.

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.

Affected Software/OS:

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

Solution:

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.

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)

References:

<https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report>

ort

<https://bettercrypto.org/>

<https://mozilla.github.io/server-side-tls/ssl-config-generator/>

<https://drownattack.com/>

<https://www.imperialviolet.org/2014/10/14/poodle.html>

CVSS Base Score: 4.3

Family name: SSL and TLS

Category: infos

Copyright: Copyright (C) 2015 SCHUTZWERK GmbH

Summary: NOSUMMARY

Version: \$Revision: 5547 \$

CVEs: CVE-2016-0800, CVE-2014-3566



Medium:

SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Risk: Medium

Application: smtp

Port: 25

Protocol: tcp

ScriptID: 111012

Vulnerability Detection Result:

In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and SSLv3 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) 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.

Summary:

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

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:N/A:N

Vulnerability Detection Method:

Check the used protocols of the services provided by this system.

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)

Affected Software/OS:

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

Solution:

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.

References:

<https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report>

ort

<https://bettercrypto.org/>

<https://mozilla.github.io/server-side-tls/ssl-config-generator/>

<https://drownattack.com/>

<https://www.imperialviolet.org/2014/10/14/poodle.html>

CVSS Base Score: 4.3

Family name: SSL and TLS

Category: infos

Copyright: Copyright (C) 2015 SCHUTZWERK GmbH

Summary: NOSUMMARY

Version: \$Revision: 5547 \$

CVEs: CVE-2016-0800, CVE-2014-3566

Medium:

SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

Risk: Medium

Application: postgres

Port: 5432

Protocol: tcp

ScriptID: 105042

Affected Software/OS:

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

Solution:

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

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.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:N

Summary:

OpenSSL is prone to security-bypass vulnerability.

Vulnerability Detection Method:

Send two SSL ChangeCipherSpec request and check the response.

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.

References:

<https://www.openssl.org/news/secadv/20140605.txt>

<http://www.securityfocus.com/bid/67899>

CVSS Base Score: 5.8

Family name: SSL and TLS

Category: attack

Copyright: This script is Copyright (C) 2014 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-10-02T07:08:50+0000

CVEs: CVE-2014-0224

Medium:

Telnet Unencrypted Cleartext Logins

Risk: Medium

Application: telnet

Port: 23

Protocol: tcp

ScriptID: 108522

Summary:

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

CVSS Base Vector:

AV:A/AC:L/Au:N/C:P/I:P/A:N

Impact:

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

Solution:

Replace Telnet with a protocol like SSH which supports encrypted connections.

CVSS Base Score: 4.8

Family name: General

Category: unknown

Copyright: Copyright (C) 2018 Greenbone Networks GmbH

Version: 2019-06-06T07:39:31+0000

Medium:

TWiki < 6.1.0 XSS Vulnerability

Risk: Medium

Application: http

Port: 80

Protocol: tcp

ScriptID: 141830

Vulnerability Detection Result:

Installed version: 01.Feb.2003

Fixed version: 6.1.0

Summary:

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

CVSS Base Vector:

AV:N/AC:M/Au:N/C:N/I:P/A:N

Vulnerability Detection Method:

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

Affected Software/OS:

TWiki version 6.0.2 and probably prior.

Solution:

Update to version 6.1.0 or later.

References:

<https://seclists.org/fulldisclosure/2019/Jan/7>

<http://twiki.org/cgi-bin/view/Codev/DownloadTWiki>

CVSS Base Score: 4.3

Family name: Web application abuses

Category: unknown

Copyright: This script is Copyright (C) 2019 Greenbone Networks GmbH

Version: 2019-03-26T08:16:24+0000

CVEs: CVE-2018-20212

Medium:

#### TWiki Cross-Site Request Forgery Vulnerability

Risk: Medium

Application: http

Port: 80

Protocol: tcp

ScriptID: 800400

Vulnerability Detection Result:

Installed version: 01.Feb.2003

Fixed version: 4.3.1

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.

Solution:

Upgrade to version 4.3.1 or later.

Affected Software/OS:

TWiki version prior to 4.3.1

Impact:

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

Summary:

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

CVSS Base Vector:

AV:N/AC:M/Au:S/C:P/I:P/A:P

References:

<http://secunia.com/advisories/34880>

<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258>

<http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-diff-cve-2009-1339.txt>

CVSS Base Score: 6.0

Family name: Web application abuses

Category: infos

Copyright: Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12952 \$

CVEs: CVE-2009-1339

Medium:

TWiki Cross-Site Request Forgery Vulnerability - Sep10

Risk: Medium

Application: http

Port: 80

Protocol: tcp

ScriptID: 801281

Vulnerability Detection Result:

Installed version: 01.Feb.2003

Fixed version: 4.3.2

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.

Affected Software/OS:

TWiki version prior to 4.3.2

Solution:

Upgrade to TWiki version 4.3.2 or later.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Summary:

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

Impact:

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

References:

<http://www.openwall.com/lists/oss-security/2010/08/03/8>

<http://www.openwall.com/lists/oss-security/2010/08/02/17>

<http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix>

<http://twiki.org/cgi-bin/view/Codev/DownloadTWiki>

CVSS Base Score: 6.8

Family name: Web application abuses

Category: infos

Copyright: Copyright (C) 2010 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12952 \$

CVEs: CVE-2009-4898

Medium:

Ubuntu Update for apache2 USN-1259-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840798

Vulnerability Detection Result:

Vulnerable package: apache2.2-common

Installed version: 2.2.8-1ubuntu0.15

Fixed version: 2.2.8-1ubuntu0.22

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 web servers 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.

Affected Software/OS:

apache2 on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:N/A:N

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1259-1

References:

<http://www.ubuntu.com/usn/usn-1259-1/>

USN:1259-1

CVSS Base Score: 5.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$



Medium:

Ubuntu Update for apache2 USN-1368-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840900

Vulnerability Detection Result:

Vulnerable package: apache2.2-common

Installed version: 2.2.8-1ubuntu0.15

Fixed version: 2.2.8-1ubuntu0.23

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 web servers behind the proxy that were not intended for external exposure. (CVE-2011-4317)

Rainer Canavan discovered that the mod\_log\_config module incorrectly handled a certain format string when used with a threaded MPM. A remote attacker could exploit this to cause a denial of service via a specially-crafted cookie. This issue only affected Ubuntu 11.04 and 11.10. (CVE-2012-0021)

It was discovered that the Apache HTTP Server incorrectly handled certain type fields within a scoreboard shared memory segment. A local attacker could exploit this to cause a denial of service. (CVE-2012-0031)

Norman Hippert discovered that the Apache HTTP Server incorrectly handled header information when returning a Bad Request (400) error page. A remote attacker could exploit this to obtain the values of certain HTTPOnly cookies. (CVE-2012-0053)

Affected Software/OS:

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

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:L/AC:L/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1368-1

References:

<http://www.ubuntu.com/usn/usn-1368-1/>

USN:1368-1

CVSS Base Score: 4.6

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY



Version: 2019-08-06T11:17:21+0000

CVEs: CVE-2011-3607, CVE-2011-4317, CVE-2012-0021, CVE-2012-0031, CVE-2012-0053

Medium:

Ubuntu Update for apache2 USN-1765-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841365

Vulnerability Detection Result:

Vulnerable package: apache2.2-common

Installed version: 2.2.8-1ubuntu0.15

Fixed version: 2.2.8-1ubuntu0.25

Affected Software/OS:

apache2 on Ubuntu 12.10,

Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

Insight:

Niels Heinen discovered that multiple modules incorrectly sanitized certain strings, which could result in browsers becoming vulnerable to cross-site scripting attacks when processing the output. With cross-site scripting vulnerabilities, if a user were tricked into viewing server output during a crafted server request, a remote attacker could exploit this to modify the contents, or steal confidential data (such as passwords), within the same domain. (CVE-2012-3499, CVE-2012-4558)

It was discovered that the mod\_proxy\_ajp module incorrectly handled error states. A remote attacker could use this issue to cause the server to stop responding, resulting in a denial of service. This issue only applied to Ubuntu 8.04 LTS, Ubuntu 10.04 LTS and Ubuntu 11.10. (CVE-2012-4557)

It was discovered that the apache2ctl script shipped in Ubuntu packages incorrectly created the lock directory. A local attacker could possibly use this issue to gain privileges. The symlink protections in Ubuntu 11.10 and later should reduce this vulnerability to a denial of service.

(CVE-2013-1048)

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:P

Summary:

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

References:

<http://www.ubuntu.com/usn/usn-1765-1/>

USN:1765-1

CVSS Base Score: 5.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2013 Greenbone Networks GmbH

Summary: Check for the Version of apache2

Version: \$Revision: 14132 \$

CVEs: CVE-2012-3499, CVE-2012-4558, CVE-2012-4557, CVE-2013-1048

Medium:

Ubuntu Update for apr USN-1134-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840667

Vulnerability Detection Result:

Vulnerable package: libapr1

Installed version: 1.2.11-1

Fixed version: 1.2.11-1ubuntu0.2

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)  
It 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)

Solution:

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

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1134-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:N/I:N/A:P

References:

<http://www.ubuntu.com/usn/usn-1134-1/>

USN:1134-1

CVSS Base Score: 4.3

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-0419, CVE-2011-1928

Medium:

Ubuntu Update for bzip2 USN-1308-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840839

Vulnerability Detection Result:

Vulnerable package: bzip2

Installed version: 1.0.4-2ubuntu4

Fixed version: 1.0.4-2ubuntu4.2

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1308-1

CVSS Base Vector:

AV:L/AC:L/Au:N/C:P/I:P/A:P

Affected Software/OS:

bzip2 on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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.

References:

<http://www.ubuntu.com/usn/usn-1308-1/>

USN:1308-1

CVSS Base Score: 4.6

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-4089

Medium:

Ubuntu Update for curl USN-1801-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841402

Vulnerability Detection Result:

Vulnerable package: curl

Installed version: 7.18.0-1ubuntu2.3

Fixed version: 7.18.0-1ubuntu2.4

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:N/A:N

Summary:

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

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 web servers.

Solution:

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

References:

USN:1801-1

<http://www.ubuntu.com/usn/usn-1801-1/>

CVSS Base Score: 5.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2013 Greenbone Networks GmbH

Summary: Check for the Version of curl

Version: \$Revision: 14132 \$

CVEs: CVE-2013-1944

Medium:

Ubuntu Update for dbus USN-1576-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841153

Vulnerability Detection Result:

Vulnerable package: libdbus-1-3

Installed version: 1.1.20-1ubuntu1

Fixed version: 1.1.20-1ubuntu3.7

CVSS Base Vector:

AV:L/AC:M/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1576-1

Solution:

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

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.

References:

<http://www.ubuntu.com/usn/usn-1576-1/>

USN:1576-1

CVSS Base Score: 6.9

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-3524

Medium:

Ubuntu Update for dbus USN-1576-2

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841177

Vulnerability Detection Result:

Vulnerable package: libdbus-1-3

Installed version: 1.1.20-1ubuntu1

Fixed version: 1.1.20-1ubuntu3.9

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.

Affected Software/OS:

dbus on Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 11.04,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:L/AC:M/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1576-2

References:

<http://www.ubuntu.com/usn/usn-1576-2/>

USN:1576-2

CVSS Base Score: 6.9

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-3524

Medium:

Ubuntu Update for eglibc USN-1589-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841171

Vulnerability Detection Result:

Vulnerable package: libc6

Installed version: 2.7-10ubuntu5

Fixed version: 2.7-10ubuntu8.2

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(), strtodf() 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)

Solution:

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

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1589-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

References:

<http://www.ubuntu.com/usn/usn-1589-1/>

USN:1589-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-3404, CVE-2012-3405, CVE-2012-3406, CVE-2012-3480



Medium:

Ubuntu Update for expat USN-1527-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841101

Vulnerability Detection Result:

Vulnerable package: libexpat1

Installed version: 2.0.1-0ubuntu1

Fixed version: 2.0.1-0ubuntu1.2

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)

Affected Software/OS:

expat on Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 11.04,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1527-1

References:

<http://www.ubuntu.com/usn/usn-1527-1/>

USN:1527-1

CVSS Base Score: 5.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-0876, CVE-2012-1148

Medium:

Ubuntu Update for freetype USN-1686-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841275

Vulnerability Detection Result:

Vulnerable package: libfreetype6

Installed version: 2.3.5-1ubuntu4.8.04.2

Fixed version: 2.3.5-1ubuntu4.8.04.10

CVSS Base Vector:

AV:N/AC:M/Au:N/C:N/I:N/A:P

Summary:

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

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.

Solution:

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

References:

<http://www.ubuntu.com/usn/usn-1686-1/>

USN:1686-1

CVSS Base Score: 4.3

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2013 Greenbone Networks GmbH

Summary: Check for the Version of freetype

Version: \$Revision: 14132 \$

CVEs: CVE-2012-5668, CVE-2012-5669, CVE-2012-5670

Medium:

Ubuntu Update for fuse vulnerability USN-1045-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840568

Vulnerability Detection Result:

Vulnerable package: fuse-utils

Installed version: 2.7.2-1ubuntu2

Fixed version: 2.7.2-1ubuntu2.2

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1045-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:N/I:P/A:P

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.

Affected Software/OS:

fuse vulnerability on Ubuntu 8.04 LTS,

Ubuntu 9.10,

Ubuntu 10.04 LTS,

Ubuntu 10.10

Solution:

Please Install the Updated Packages.

References:

<http://www.ubuntu.com/usn/usn-1045-1/>

USN:1045-1

CVSS Base Score: 5.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2010-3879

Medium:

Ubuntu Update for glibc USN-1589-2

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841254

Vulnerability Detection Result:

Vulnerable package: libc6

Installed version: 2.7-10ubuntu5

Fixed version: 2.7-10ubuntu8.3

Affected Software/OS:

glibc on Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

Insight:

USN-1589-1 fixed vulnerabilities in the GNU C Library. One of the updates exposed a regression in the floating point parser. This update fixes the problem.

We apologize for the inconvenience.

Original advisory details:

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

It was discovered that multiple integer overflows existed in the strtod(), strtodf() 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)

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1589-2

References:

<http://www.ubuntu.com/usn/usn-1589-2/>

USN:1589-2

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-3404, CVE-2012-3405, CVE-2012-3406, CVE-2012-3480

Medium:

Ubuntu Update for gnupg USN-1570-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841152

Vulnerability Detection Result:

Vulnerable package: gnupg

Installed version: 1.4.6-2ubuntu5

Fixed version: 1.4.6-2ubuntu5.1

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1570-1

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:P/A:N

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.

Solution:

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

References:

<http://www.ubuntu.com/usn/usn-1570-1/>

USN:1570-1

CVSS Base Score: 5.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

Medium:

Ubuntu Update for gnupg USN-1682-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841270

Vulnerability Detection Result:

Vulnerable package: gnupg

Installed version: 1.4.6-2ubuntu5

Fixed version: 1.4.6-2ubuntu5.2

Affected Software/OS:

gnupg on Ubuntu 12.10,

Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:N/I:P/A:P

Summary:

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

References:

<http://www.ubuntu.com/usn/usn-1682-1/>

USN:1682-1

CVSS Base Score: 5.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2013 Greenbone Networks GmbH

Summary: Check for the Version of gnupg

Version: \$Revision: 14132 \$

CVEs: CVE-2012-6085

Medium:

Ubuntu Update for gnutls26 USN-1418-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840978

Vulnerability Detection Result:

Vulnerable package: libgnutls13

Installed version: 2.0.4-1ubuntu2

Fixed version: 2.0.4-1ubuntu2.7

Solution:

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

Insight:

Alban Crequy discovered that the GnuTLS library incorrectly checked array bounds when copying TLS session data. A remote attacker could crash a client application, leading to a denial of service, as the client application prepared for TLS session resumption. (CVE-2011-4128)

Matthew Hall discovered that the GnuTLS library incorrectly handled TLS records. A remote attacker could crash client and server applications, leading to a denial of service, by sending a crafted TLS record. (CVE-2012-1573)

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1418-1

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

<http://www.ubuntu.com/usn/usn-1418-1/>

USN:1418-1

CVSS Base Score: 5.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-4128, CVE-2012-1573

Medium:

Ubuntu Update for gnutls26 USN-1752-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841340

Vulnerability Detection Result:

Vulnerable package: libgnutls13

Installed version: 2.0.4-1ubuntu2

Fixed version: 2.0.4-1ubuntu2.9

Summary:

The remote host is missing an update for the 'gnutls26' package(s) announced via the referenced advisory.

CVSS Base Vector:

AV:N/AC:H/Au:N/C:P/I:P/A:N

Affected Software/OS:

gnutls26 on Ubuntu 12.10,

Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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.

References:

<http://www.ubuntu.com/usn/usn-1752-1/>

USN:1752-1

CVSS Base Score: 4.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2013 Greenbone Networks GmbH

Summary: Check for the Version of gnutls26

Version: \$Revision: 14132 \$

CVEs: CVE-2013-1619



Medium:

Ubuntu Update for libgc USN-1546-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841125

Vulnerability Detection Result:

Vulnerable package: libgc1c2

Installed version: 6.8-1.1

Fixed version: 1:6.8-1.1ubuntu0.1

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.

Affected Software/OS:

libgc on Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 11.04,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:P/A:N

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1546-1

References:

<http://www.ubuntu.com/usn/usn-1546-1/>

USN:1546-1

CVSS Base Score: 5.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-2673

Medium:

Ubuntu Update for libpng USN-1175-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840714

Vulnerability Detection Result:

Vulnerable package: libpng12-0

Installed version: 1.2.15~beta5-3ubuntu0.2

Fixed version: 1.2.15~beta5-3ubuntu0.4

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1175-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Affected Software/OS:

libpng on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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)

References:

<http://www.ubuntu.com/usn/usn-1175-1/>

USN:1175-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-2501, CVE-2011-2690, CVE-2011-2692

Medium:

Ubuntu Update for libpng USN-1402-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840960

Vulnerability Detection Result:

Vulnerable package: libpng12-0

Installed version: 1.2.15~beta5-3ubuntu0.2

Fixed version: 1.2.15~beta5-3ubuntu0.6

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1402-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

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.

Solution:

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

References:

<http://www.ubuntu.com/usn/usn-1402-1/>

USN:1402-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-3045

Medium:

Ubuntu Update for libpng USN-1417-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840979

Vulnerability Detection Result:

Vulnerable package: libpng12-0

Installed version: 1.2.15~beta5-3ubuntu0.2

Fixed version: 1.2.15~beta5-3ubuntu0.7

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1417-1

Solution:

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

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.

References:

<http://www.ubuntu.com/usn/usn-1417-1/>

USN:1417-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-3048

Medium:

Ubuntu Update for libtasn1-3 USN-1436-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840994

Vulnerability Detection Result:

Vulnerable package: libtasn1-3

Installed version: 1.1-1

Fixed version: 1.1-1ubuntu0.1

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1436-1

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:P

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.

Affected Software/OS:

libtasn1-3 on Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 11.04,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

References:

<http://www.ubuntu.com/usn/usn-1436-1/>

USN:1436-1

CVSS Base Score: 5.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-1569

Medium:

Ubuntu Update for libxml2 USN-1376-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840917

Vulnerability Detection Result:

Vulnerable package: libxml2

Installed version: 2.6.31.dfsg-2ubuntu1

Fixed version: 2.6.31.dfsg-2ubuntu1.8

Solution:

Please Install the Updated Packages.

Affected Software/OS:

libxml2 on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1376-1

References:

<http://www.ubuntu.com/usn/usn-1376-1/>

USN:1376-1

CVSS Base Score: 5.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-0841

Medium:

Ubuntu Update for libxml2 USN-1447-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841007

Vulnerability Detection Result:

Vulnerable package: libxml2

Installed version: 2.6.31.dfsg-2ubuntu1

Fixed version: 2.6.31.dfsg-2ubuntu1.9

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.

Solution:

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

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1447-1

References:

<http://www.ubuntu.com/usn/usn-1447-1/>

USN:1447-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-3102

Medium:

Ubuntu Update for libxml2 USN-1587-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841166

Vulnerability Detection Result:

Vulnerable package: libxml2

Installed version: 2.6.31.dfsg-2ubuntu1

Fixed version: 2.6.31.dfsg-2ubuntu1.10

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1587-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Solution:

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

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.

References:

<http://www.ubuntu.com/usn/usn-1587-1/>

USN:1587-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-2807



Medium:

Ubuntu Update for libxml2 USN-1656-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841242

Vulnerability Detection Result:

Vulnerable package: libxml2

Installed version: 2.6.31.dfsg-2ubuntu1

Fixed version: 2.6.31.dfsg-2ubuntu1.11

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1656-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

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.

Affected Software/OS:

libxml2 on Ubuntu 12.10,

Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

References:

<http://www.ubuntu.com/usn/usn-1656-1/>

USN:1656-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-5134

Medium:

Ubuntu Update for libxml2 USN-1782-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841380

Vulnerability Detection Result:

Vulnerable package: libxml2

Installed version: 2.6.31.dfsg-2ubuntu1

Fixed version: 2.6.31.dfsg-2ubuntu1.12

Summary:

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

CVSS Base Vector:

AV:N/AC:M/Au:N/C:N/I:N/A:P

Solution:

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

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.

References:

<http://www.ubuntu.com/usn/usn-1782-1/>

USN:1782-1

CVSS Base Score: 4.3

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2013 Greenbone Networks GmbH

Summary: Check for the Version of libxml2

Version: \$Revision: 14132 \$

CVEs: CVE-2013-0338

Medium:

Ubuntu Update for logrotate USN-1172-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840705

Vulnerability Detection Result:

Vulnerable package: logrotate

Installed version: 3.7.1-3

Fixed version: 3.7.1-3ubuntu0.8.04.1

Insight:

It was discovered that logrotate incorrectly handled the creation of new log files. Local users could possibly read log files if they were opened before permissions were in place. This issue only affected Ubuntu 8.04 LTS. (CVE-2011-1098)

It was discovered that logrotate incorrectly handled certain log file names when used with the shred option. Local attackers able to create log files with specially crafted filenames could use this issue to execute arbitrary code. This issue only affected Ubuntu 10.04 LTS, 10.10, and 11.04. (CVE-2011-1154)

It was discovered that logrotate incorrectly handled certain malformed log filenames. Local attackers able to create log files with specially crafted filenames could use this issue to cause logrotate to stop processing log files, resulting in a denial of service. (CVE-2011-1155)

It was discovered that logrotate incorrectly handled symlinks and hard links when processing log files. A local attacker having write access to a log file directory could use this issue to overwrite or read arbitrary files. This issue only affected Ubuntu 8.04 LTS. (CVE-2011-1548)

Affected Software/OS:

logrotate on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:L/AC:M/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1172-1

References:

<http://www.ubuntu.com/usn/usn-1172-1/>

USN:1172-1

CVSS Base Score: 6.9

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-1098, CVE-2011-1154, CVE-2011-1155, CVE-2011-1548

Medium:

Ubuntu Update for mysql-5.1 USN-1427-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840989

Vulnerability Detection Result:

Vulnerable package: mysql-server-5.0

Installed version: 5.0.51a-3ubuntu5

Fixed version: 5.0.96-0ubuntu1

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1427-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Affected Software/OS:

mysql-5.1 on Ubuntu 11.10,

Ubuntu 11.04,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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.

References:

<http://www.ubuntu.com/usn/usn-1427-1/>

USN:1427-1

<http://dev.mysql.com/doc/refman/5.1/en/news-5-1-62.html>

<http://dev.mysql.com/doc/refman/5.0/en/news-5-0-96.html>

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

Medium:

Ubuntu Update for mysql-5.5 USN-1467-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841039

Vulnerability Detection Result:

Vulnerable package: mysql-server-5.0

Installed version: 5.0.51a-3ubuntu5

Fixed version: 5.0.96-0ubuntu3

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

Solution:

Please Install the Updated Packages.

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.

CVSS Base Vector:

AV:N/AC:H/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1467-1

References:

<http://www.ubuntu.com/usn/usn-1467-1/>

USN:1467-1

<http://dev.mysql.com/doc/refman/5.5/en/news-5-5-24.html>

<http://dev.mysql.com/doc/refman/5.1/en/news-5-1-63.html>

CVSS Base Score: 5.1

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-2122

Medium:

Ubuntu Update for openldap, openldap2.3 vulnerabilities USN-1100-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840624

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

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)

Affected Software/OS:

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

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1100-1

References:

<http://www.ubuntu.com/usn/usn-1100-1/>

USN:1100-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-1024, CVE-2011-1025, CVE-2011-1081

Medium:

Ubuntu Update for openssl USN-1451-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841013

Vulnerability Detection Result:

Vulnerable package: libssl0.9.8

Installed version: 0.9.8g-4ubuntu3.18

Fixed version: 0.9.8g-4ubuntu3.19

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1451-1

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)

Solution:

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

References:

<http://www.ubuntu.com/usn/usn-1451-1/>

USN:1451-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-0884, CVE-2012-2333

Medium:

Ubuntu Update for openssl USN-1732-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841327

Vulnerability Detection Result:

Vulnerable package: libssl0.9.8

Installed version: 0.9.8g-4ubuntu3.18

Fixed version: 0.9.8g-4ubuntu3.20

Affected Software/OS:

openssl on Ubuntu 12.10,

Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

Insight:

Adam Langley and Wolfgang Ertl 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)

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:P

Summary:

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

References:

<http://www.ubuntu.com/usn/usn-1732-1/>

USN:1732-1

CVSS Base Score: 5.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2013 Greenbone Networks GmbH

Summary: Check for the Version of openssl

Version: \$Revision: 14132 \$

CVEs: CVE-2012-2686, CVE-2013-0166, CVE-2013-0169



Medium:

Ubuntu Update for pam USN-1140-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840672

Vulnerability Detection Result:

Vulnerable package: libpam-modules

Installed version: 0.99.7.1-5ubuntu6

Fixed version: 0.99.7.1-5ubuntu6.3

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)

Solution:

Please Install the Updated Packages.

Affected Software/OS:

pam on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1140-1

CVSS Base Vector:

AV:L/AC:M/Au:N/C:C/I:C/A:C

References:

<http://www.ubuntu.com/usn/usn-1140-1/>

USN:1140-1

CVSS Base Score: 6.9

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2009-0887, CVE-2010-3316, CVE-2010-3430, CVE-2010-3431, CVE-2010-3435, CVE-2010-3853, CVE-2010-4706, CVE-2010-4707

Medium:

Ubuntu Update for pam USN-1140-2

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840673

Vulnerability Detection Result:

Vulnerable package: libpam-modules

Installed version: 0.99.7.1-5ubuntu6

Fixed version: 0.99.7.1-5ubuntu6.4

Insight:

USN-1140-1 fixed vulnerabilities in PAM. A regression was found that caused cron to stop working with a 'Module is unknown' error. As a result, systems configured with automatic updates will not receive updates until cron is restarted, these updates are installed or the system is rebooted. This update fixes the problem.

We apologize for the inconvenience.

Original advisory details:

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

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

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

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

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)

Solution:

Please Install the Updated Packages.

Affected Software/OS:

pam on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

CVSS Base Vector:

AV:L/AC:M/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1140-2

References:

<http://www.ubuntu.com/usn/usn-1140-2/>

USN:1140-2

CVSS Base Score: 6.9

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2009-0887, CVE-2010-3316, CVE-2010-3430, CVE-2010-3431, CVE-2010-3435, CVE-2010-3853, CVE-2010-4706, CVE-2010-4707

Medium:

Ubuntu Update for pam USN-1237-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840794

Vulnerability Detection Result:

Vulnerable package: libpam-modules

Installed version: 0.99.7.1-5ubuntu6

Fixed version: 0.99.7.1-5ubuntu6.5

Solution:

Please Install the Updated Packages.

Affected Software/OS:

pam on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Insight:

Kees Cook discovered that the PAM pam\_env module incorrectly handled certain malformed environment files. A local attacker could use this flaw to cause a denial of service, or possibly gain privileges. The default compiler options for affected releases should reduce the vulnerability to a denial of service. (CVE-2011-3148)

Kees Cook discovered that the PAM pam\_env module incorrectly handled variable expansion. A local attacker could use this flaw to cause a denial of service. (CVE-2011-3149)

Stephane Chazelas discovered that the PAM pam\_motd module incorrectly cleaned the environment during execution of the motd scripts. In certain environments, a local attacker could use this to execute arbitrary code as root, and gain privileges.

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1237-1

CVSS Base Vector:

AV:L/AC:M/Au:N/C:C/I:C/A:C

References:

<http://www.ubuntu.com/usn/usn-1237-1/>

USN:1237-1

CVSS Base Score: 6.9

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-3148, CVE-2011-3149, CVE-2011-3628

Medium:

Ubuntu Update for php5 regression USN-1042-2

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840566

Vulnerability Detection Result:

Vulnerable package: php5-cgi

Installed version: 5.2.4-2ubuntu5.10

Fixed version: 5.2.4-2ubuntu5.14

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:P/A:N

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1042-2

Solution:

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

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)

References:

<http://www.ubuntu.com/usn/usn-1042-2/>

USN:1042-2

CVSS Base Score: 5.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2010-3436

Medium:

Ubuntu Update for php5 USN-1307-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840842

Vulnerability Detection Result:

Vulnerable package: php5-cgi

Installed version: 5.2.4-2ubuntu5.10

Fixed version: 5.2.4-2ubuntu5.19

Affected Software/OS:

php5 on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:N/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1307-1

References:

<http://www.ubuntu.com/usn/usn-1307-1/>

USN:1307-1

CVSS Base Score: 6.4

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-4566

## Medium:

Ubuntu Update for php5 vulnerabilities USN-1042-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840564

Vulnerability Detection Result:

Vulnerable package: php5-cgi

Installed version: 5.2.4-2ubuntu5.10

Fixed version: 5.2.4-2ubuntu5.13

Insight:

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

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

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

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

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

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

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

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

Solution:

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

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1042-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

References:

<http://www.ubuntu.com/usn/usn-1042-1/>

USN:1042-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-09-16T06:54:58+0000

CVEs: CVE-2009-5016, CVE-2010-3436, CVE-2010-3709, CVE-2010-3710, CVE-2010-3870, CVE-2010-4156, CVE-2010-4409, CVE-2010-4645



Medium:

Ubuntu Update for postfix USN-1113-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840648

Vulnerability Detection Result:

Vulnerable package: postfix

Installed version: 2.5.1-2ubuntu1

Fixed version: 2.5.1-2ubuntu1.3

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1113-1

CVSS Base Vector:

AV:L/AC:M/Au:N/C:C/I:C/A:C

Affected Software/OS:

postfix on Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 9.10,

Ubuntu 8.04 LTS,

Ubuntu 6.06 LTS

Solution:

Please Install the Updated Packages.

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)

References:

<http://www.ubuntu.com/usn/usn-1113-1/>

USN:1113-1

CVSS Base Score: 6.9

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2009-2939, CVE-2011-0411

Medium:

Ubuntu Update for postfix USN-1131-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840658

Vulnerability Detection Result:

Vulnerable package: postfix

Installed version: 2.5.1-2ubuntu1

Fixed version: 2.5.1-2ubuntu1.4

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1131-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

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.

Affected Software/OS:

postfix on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS,

Ubuntu 6.06 LTS

Solution:

Please Install the Updated Packages.

References:

<http://www.ubuntu.com/usn/usn-1131-1/>

USN:1131-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-1720

Medium:

Ubuntu Update for PostgreSQL vulnerability USN-1058-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840577

Vulnerability Detection Result:

Vulnerable package: libpq5

Installed version: 8.3.1-1

Fixed version: 8.3.14-0ubuntu8.04

Affected Software/OS:

PostgreSQL vulnerability on Ubuntu 6.06 LTS,

Ubuntu 8.04 LTS,

Ubuntu 9.10,

Ubuntu 10.04 LTS,

Ubuntu 10.10

Solution:

Please Install the Updated Packages.

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.

CVSS Base Vector:

AV:N/AC:L/Au:S/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1058-1

References:

<http://www.ubuntu.com/usn/usn-1058-1/>

USN:1058-1

CVSS Base Score: 6.5

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2010-4015

Medium:

Ubuntu Update for postgresql-8.4 USN-1229-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840772

Vulnerability Detection Result:

Vulnerable package: postgresql-8.3

Installed version: 8.3.1-1

Fixed version: 8.3.16-0ubuntu0.8.04

Solution:

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

Insight:

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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:N/A:N

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1229-1

References:

<http://www.ubuntu.com/usn/usn-1229-1/>

USN:1229-1

CVSS Base Score: 5.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-2483

Medium:

Ubuntu Update for postgresql-9.1 USN-1378-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840921

Vulnerability Detection Result:

Vulnerable package: postgresql-8.3

Installed version: 8.3.1-1

Fixed version: 8.3.18-0ubuntu0.8.04

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1378-1

Solution:

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

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)

References:

<http://www.ubuntu.com/usn/usn-1378-1/>

USN:1378-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-0866, CVE-2012-0867, CVE-2012-0868

Medium:

Ubuntu Update for postgresql-9.1 USN-1461-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841032

Vulnerability Detection Result:

Vulnerable package: postgresql-8.3

Installed version: 8.3.1-1

Fixed version: 8.3.19-0ubuntu8.04

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1461-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:N/I:P/A:N

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

Solution:

Please Install the Updated Packages.

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)

References:

<http://www.ubuntu.com/usn/usn-1461-1/>

USN:1461-1

CVSS Base Score: 4.3

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-2143, CVE-2012-2655

Medium:

Ubuntu Update for postgresql-9.1 USN-1542-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841120

Vulnerability Detection Result:

Vulnerable package: postgresql-8.3

Installed version: 8.3.1-1

Fixed version: 8.3.20-0ubuntu8.04

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)

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

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:N/AC:M/Au:S/C:P/I:P/A:N

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1542-1

References:

<http://www.ubuntu.com/usn/usn-1542-1/>

USN:1542-1

CVSS Base Score: 4.9

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-3488, CVE-2012-3489

Medium:

Ubuntu Update for postgresql-9.1 USN-1717-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841317

Vulnerability Detection Result:

Vulnerable package: postgresql-8.3

Installed version: 8.3.1-1

Fixed version: 8.3.23-0ubuntu8.04

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

Solution:

Please Install the Updated Packages.

Insight:

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

CVSS Base Vector:

AV:N/AC:L/Au:S/C:N/I:N/A:C

Summary:

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

References:

<http://www.ubuntu.com/usn/usn-1717-1/>

USN:1717-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2013 Greenbone Networks GmbH

Summary: Check for the Version of postgresql-9.1

Version: \$Revision: 14132 \$

CVEs: CVE-2013-0255



Medium:

Ubuntu Update for python2.5 USN-1613-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841195

Vulnerability Detection Result:

Vulnerable package: python2.5

Installed version: 2.5.2-2ubuntu6.1

Fixed version: 2.5.2-2ubuntu6.2

Affected Software/OS:

python2.5 on Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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 automated system were tricked into opening a crafted audio file, an attacker could cause a denial of service via application crash. (CVE-2010-1634, CVE-2010-2089)

Giampaolo Rodola discovered several race conditions in the smtpd module. A remote attacker could exploit this to cause a denial of service via daemon outage. (CVE-2010-3493)

It was discovered that the CGIHTTPServer module did not properly perform input validation on certain HTTP GET requests. A remote attacker could potentially obtain access to CGI script source files. (CVE-2011-1015)

Niels Heinen discovered that the urllib and urllib2 modules would process Location headers that specify a redirection to file: URLs. A remote attacker could exploit this to obtain sensitive information or cause a denial of service. (CVE-2011-1521)

It was discovered that SimpleHTTPServer did not use a charset parameter in the Content-Type HTTP header. An attacker could potentially exploit this to conduct cross-site scripting (XSS) attacks against Internet Explorer 7 users. (CVE-2011-4940)

It was discovered that Python distutils contained a race condition when creating the ~/.pyirc 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)

CVSS Base Vector:

AV:L/AC:M/Au:N/C:C/I:C/A:C

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1613-1

References:

<http://www.ubuntu.com/usn/usn-1613-1/>

USN:1613-1

CVSS Base Score: 6.9

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: 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

Medium:

Ubuntu Update for samba vulnerability USN-1075-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840597

Vulnerability Detection Result:

Vulnerable package: samba-common

Installed version: 3.0.20-0.1ubuntu1

Fixed version: 3.0.28a-1ubuntu4.14

Affected Software/OS:

samba vulnerability on Ubuntu 6.06 LTS,

Ubuntu 8.04 LTS,

Ubuntu 9.10,

Ubuntu 10.04 LTS,

Ubuntu 10.10

Solution:

Please Install the Updated Packages.

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1075-1

References:

<http://www.ubuntu.com/usn/usn-1075-1/>

USN:1075-1

CVSS Base Score: 5.0

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-0719

Medium:

Ubuntu Update for sudo USN-1754-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841349

Vulnerability Detection Result:

Vulnerable package: sudo

Installed version: 1.6.9p10-1ubuntu3

Fixed version: 1.6.9p10-1ubuntu3.10

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.

Affected Software/OS:

sudo on Ubuntu 12.10,

Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:L/AC:M/Au:N/C:C/I:C/A:C

Summary:

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

References:

<http://www.ubuntu.com/usn/usn-1754-1/>

USN:1754-1

CVSS Base Score: 6.9

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2013 Greenbone Networks GmbH

Summary: Check for the Version of sudo

Version: \$Revision: 14132 \$

CVEs: CVE-2013-1775

Medium:

Ubuntu Update for tiff USN-1416-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840976

Vulnerability Detection Result:

Vulnerable package: libtiff4

Installed version: 3.8.2-7ubuntu3.4

Fixed version: 3.8.2-7ubuntu3.10

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1416-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

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)

Affected Software/OS:

tiff on Ubuntu 11.10,

Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

References:

<http://www.ubuntu.com/usn/usn-1416-1/>

USN:1416-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-1173, CVE-2010-4665

Medium:

Ubuntu Update for tiff USN-1631-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841216

Vulnerability Detection Result:

Vulnerable package: libtiff4

Installed version: 3.8.2-7ubuntu3.4

Fixed version: 3.8.2-7ubuntu3.14

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)

Solution:

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

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1631-1

References:

<http://www.ubuntu.com/usn/usn-1631-1/>

USN:1631-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-4447, CVE-2012-4564

Medium:

Ubuntu Update for tiff USN-1655-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 841244

Vulnerability Detection Result:

Vulnerable package: libtiff4

Installed version: 3.8.2-7ubuntu3.4

Fixed version: 3.8.2-7ubuntu3.16

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1655-1

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

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.

Solution:

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

References:

<http://www.ubuntu.com/usn/usn-1655-1/>

USN:1655-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-5581

Medium:

Ubuntu Update for tiff vulnerability USN-1102-1

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840626

Vulnerability Detection Result:

Vulnerable package: libtiff4

Installed version: 3.8.2-7ubuntu3.4

Fixed version: 3.8.2-7ubuntu3.9

Solution:

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

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.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1102-1

References:

<http://www.ubuntu.com/usn/usn-1102-1/>

USN:1102-1

CVSS Base Score: 6.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-1167



Medium:

Ubuntu Update for update-manager USN-1284-2

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840901

Vulnerability Detection Result:

Vulnerable package: update-manager-core

Installed version: 0.87.24

Fixed version: 0.87.33

Affected Software/OS:

update-manager on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:N

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1284-2

References:

<http://www.ubuntu.com/usn/usn-1284-2/>

USN:1284-2

CVSS Base Score: 6.4

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-3152, CVE-2011-3154

Medium:

Ubuntu Update for util-linux update USN-1045-2

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 840569

Vulnerability Detection Result:

Vulnerable package: bsduutils

Installed version: 2.13.1-5ubuntu1

Fixed version: 2.13.1-5ubuntu3.1

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.

Solution:

Please Install the Updated Packages.

Affected Software/OS:

util-linux update on Ubuntu 8.04 LTS,

Ubuntu 9.10,

Ubuntu 10.04 LTS,

Ubuntu 10.10

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1045-2

CVSS Base Vector:

AV:N/AC:M/Au:N/C:N/I:P/A:P

References:

<http://www.ubuntu.com/usn/usn-1045-2/>

USN:1045-2

CVSS Base Score: 5.8

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2010-3879

Medium:

### UnrealIRCd Authentication Spoofing Vulnerability

Risk: Medium

Application: irc

Port: 6667

Protocol: tcp

ScriptID: 809883

Vulnerability Detection Result:

Installed version: 3.2.8.1

Fixed version: 3.2.10.7

Impact:

Successful exploitation of this vulnerability

will allow remote attackers to spoof certificate fingerprints and consequently log in as another user.

Summary:

This host is installed with UnrealIRCd

and is prone to authentication spoofing vulnerability.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Vulnerability Detection Method:

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

Insight:

The flaw exists due to an error in

the 'm\_authenticate' function in 'modules/m\_sasl.c' script.

Affected Software/OS:

UnrealIRCd before 3.2.10.7 and

4.x before 4.0.6.

Solution:

Upgrade to UnrealIRCd 3.2.10.7,

or 4.0.6, or later.

References:

<http://seclists.org/oss-sec/2016/q3/420>

<http://www.openwall.com/lists/oss-security/2016/09/05/8>

<https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86bc50ba1a34a766>

[https://bugs.unrealircd.org/main\\_page.php](https://bugs.unrealircd.org/main_page.php)

CVSS Base Score: 6.8

Family name: General

Category: infos

Copyright: Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 11874 \$

CVEs: CVE-2016-7144

Medium:

#### VNC Server Unencrypted Data Transmission

Risk: Medium

Application: vnc

Port: 5900

Protocol: tcp

ScriptID: 108529

Vulnerability Detection Result:

The VNC server provides the following insecure or cryptographically weak Security Type(s):

2 (VNC authentication)

Solution:

Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254].

Some VNC server vendors are also providing more secure Security Types within their products.

CVSS Base Vector:

AV:A/AC:L/Au:N/C:P/I:P/A:N

Summary:

The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.

Impact:

An attacker can uncover sensitive data by sniffing traffic to the VNC server.

References:

<https://tools.ietf.org/html/rfc6143#page-10>

CVSS Base Score: 4.8

Family name: General

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: \$Revision: 13014 \$

Medium:

FTP Unencrypted Cleartext Login

Risk: Medium

Application: unknown

Port: 2121

Protocol: tcp

ScriptID: 108528

Vulnerability Detection Result:

The remote FTP service accepts logins without a previous sent 'AUTH TLS' command. Response(s):

Anonymous sessions: 331 Password required for anonymous

Non-anonymous sessions: 331 Password required for openvas-vt

Solution:

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

Impact:

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

CVSS Base Vector:

AV:A/AC:L/Au:N/C:P/I:P/A:N

Summary:

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

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.

CVSS Base Score: 4.8

Family name: General

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: 2020-03-24T12:27:11+0000

Medium:

Check for Anonymous FTP Login

Risk: Medium

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 900600

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

Solution:

If you do not want to share files, you should disable anonymous logins.

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:P/A:N

Summary:

Reports if the remote FTP Server allows anonymous logins.

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.

References:

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

CVSS Base Score: 6.4

Family name: FTP

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2020-03-24T12:27:11+0000

Medium:

FTP Unencrypted Cleartext Login

Risk: Medium

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 108528

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.

Summary:

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

CVSS Base Vector:

AV:A/AC:L/Au:N/C:P/I:P/A:N

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.

Impact:

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

Solution:

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

CVSS Base Score: 4.8

Family name: General

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: 2020-03-24T12:27:11+0000

Medium:

Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Risk: Medium

Application: http

Port: 80

Protocol: tcp

ScriptID: 902830

Solution:

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

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.

Impact:

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

Summary:

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

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:N/A:N

References:

<http://secunia.com/advisories/47779>

<http://www.exploit-db.com/exploits/18442>

<http://rhn.redhat.com/errata/RHSA-2012-0128.html>

[http://httpd.apache.org/security/vulnerabilities\\_22.html](http://httpd.apache.org/security/vulnerabilities_22.html)

<http://svn.apache.org/viewvc?view=revision&revision=1235454>

<http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html>

CVSS Base Score: 4.3

Family name: Web Servers

Category: attack

Copyright: Copyright (C) 2012 SecPod

Summary: NOSUMMARY

Version: \$Revision: 11857 \$

CVEs: CVE-2012-0053



Medium:

HTTP Debugging Methods (TRACE/TRACK) Enabled

Risk: Medium

Application: http

Port: 80

Protocol: tcp

ScriptID: 11213

Vulnerability Detection Result:

The web server has the following HTTP methods enabled: TRACE

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.

Affected Software/OS:

Web servers with enabled TRACE and/or TRACK methods.

Solution:

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.

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:N

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.

Impact:

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

References:

<http://www.kb.cert.org/vuls/id/288308>

<http://www.kb.cert.org/vuls/id/867593>

<http://httpd.apache.org/docs/current/de/mod/core.html#traceenable>

[https://www.owasp.org/index.php/Cross\\_Site\\_Tracing](https://www.owasp.org/index.php/Cross_Site_Tracing)

CVSS Base Score: 5.8

Family name: Web application abuses

Category: unknown

Copyright: This script is Copyright (C) 2003 E-Soft Inc.

Version: 2019-11-22T13:51:04+0000

CVEs: 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

Medium:

Insecure Saving Of Downloadable File In Mozilla Firefox (Linux)

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 900869

Vulnerability Detection Result:

The target host was found to be vulnerable

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.

Affected Software/OS:

Mozilla Firefox version 2.x, 3.x on Linux.

Solution:

Upgrade to Mozilla Firefox version 3.6.3 or later

CVSS Base Vector:

AV:L/AC:M/Au:N/C:P/I:P/A:P

Summary:

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

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.

References:

<http://secunia.com/advisories/36649>

<http://jbbrownsec.blogspot.com/2009/09/vamos-updates.html>

<http://securitytube.net/Zero-Day-Demos-%28Firefox-Vulnerability-Discovered%29-video.aspx>

<http://www.mozilla.com/en-US/firefox/>

CVSS Base Score: 4.4

Family name: General

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2019-12-05T15:10:00+0000

CVEs: CVE-2009-3274

Medium:

Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability

Risk: Medium

Application: smtp

Port: 25

Protocol: tcp

ScriptID: 103935

Summary:

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

CVSS Base Vector:

AV:N/AC:M/Au:N/C:P/I:P/A:P

Vulnerability Detection Method:

Send a special crafted 'STARTTLS' request and check the response.

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.

Affected Software/OS:

The following vendors are affected:

Ipswitch

Kerio

Postfix

Qmail-TLS

Oracle

SCO Group

spamdyke

ISC

Solution:

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

References:

<http://www.securityfocus.com/bid/46767>

<http://kolab.org/pipermail/kolab-announce/2011/000101.html>

[http://bugzilla.cyrusimap.org/show\\_bug.cgi?id=3424](http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424)

[http://cyrusimap.org/mediawiki/index.php/Bugs\\_Resolved\\_in\\_2.4.7](http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7)

<http://www.kb.cert.org/vuls/id/MAPG-8D9M4P>

<http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-notes.txt>

<http://www.postfix.org/CVE-2011-0411.html>

<http://www.pureftpd.org/project/pure-ftpd/news>

[http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN\\_ReleaseNotes\\_XCS\\_9\\_1\\_1/EN\\_ReleaseNotes\\_WG\\_XCS\\_9\\_1\\_TLS\\_Hotfix.pdf](http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf)

<http://www.spamdyke.org/documentation/Changelog.txt>

[http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?include\\_text=1](http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?include_text=1)

<http://www.securityfocus.com/archive/1/516901>

<http://support.avaya.com/css/P8/documents/100134676>

<http://support.avaya.com/css/P8/documents/100141041>

<http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>

<http://inoa.net/qmail-tls/vu555316.patch>

<http://www.kb.cert.org/vuls/id/555316>

CVSS Base Score: 6.8

Family name: SMTP problems

Category: attack

Copyright: This script is Copyright (C) 2014 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-23T13:51:29+0000

CVEs: CVE-2011-0411, CVE-2011-1430, CVE-2011-1431, CVE-2011-1432, CVE-2011-1506, CVE-2011-1575,  
CVE-2011-1926, CVE-2011-2165

Medium:

phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Risk: Medium

Application: http

Port: 80

Protocol: tcp

ScriptID: 801660

Affected Software/OS:

phpMyAdmin version 3.3.8.1 and prior.

Solution:

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.

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.

Impact:

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

CVSS Base Vector:

AV:N/AC:M/Au:N/C:N/I:P/A:N

Summary:

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

References:

<http://www.exploit-db.com/exploits/15699/>

<http://www.vupen.com/english/advisories/2010/3133>

CVSS Base Score: 4.3

Family name: Web application abuses

Category: attack

Copyright: Copyright (C) 2010 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-12-05T15:10:00+0000

CVEs: CVE-2010-4480

Medium:

Pidgin MSN Protocol Plugin Denial Of Service Vulnerability (Linux)

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 800424

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.

Summary:

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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:P

Affected Software/OS:

Pidgin version prior to 2.6.6 on Linux.

Solution:

Upgrade to Pidgin version 2.6.6 or later.

Insight:

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

References:

<http://www.openwall.com/lists/oss-security/2010/01/07/2>

CVSS Base Score: 5.0

Family name: Denial of Service

Category: infos

Copyright: Copyright (c) 2010 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12670 \$

CVEs: CVE-2010-0277

Medium:

awiki Multiple Local File Include Vulnerabilities

Risk: Medium

Application: http

Port: 80

Protocol: tcp

ScriptID: 103210

Vulnerability Detection Result:

Vulnerable url: <http://192.168.56.12/mutillidae/index.php?page=/etc/passwd>

Affected Software/OS:

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

Solution:

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.

Impact:

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.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:N/A:N

Summary:

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

References:

<https://www.exploit-db.com/exploits/36047/>

<http://www.securityfocus.com/bid/49187>

<http://www.kobaonline.com/awiki/>

CVSS Base Score: 5.0

Family name: Web application abuses

Category: attack

Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-12-11T11:26:13+0000

Medium:

## Pidgin Multiple Denial Of Service Vulnerabilities (Linux)

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 900941

Vulnerability Detection Result:

Installed version: 2.5.2

Fixed version: 2.6.2

Summary:

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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:P

Impact:

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

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.

Solution:

Upgrade to Pidgin version 2.6.2.

Affected Software/OS:

Pidgin version prior to 2.6.2 on Linux.

References:

<http://secunia.com/advisories/36601>

<http://developer.pidgin.im/ticket/10159>

<http://www.pidgin.im/news/security/?id=37>

<http://www.pidgin.im/news/security/?id=38>

<http://www.pidgin.im/news/security/?id=39>

<http://www.pidgin.im/news/security/?id=40>

CVSS Base Score: 5.0

Family name: Denial of Service

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: \$Revision: 12670 \$

CVEs: CVE-2009-2703, CVE-2009-3083, CVE-2009-3084, CVE-2009-3085



Medium:

Pidgin OSCAR Protocol Denial Of Service Vulnerability (Linux)

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 800824

Vulnerability Detection Result:

Installed version: 2.5.2

Fixed version: 2.5.8

Summary:

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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:P

Impact:

Successful exploitation will allow attacker to cause a application crash.

Insight:

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

Solution:

Upgrade to Pidgin version 2.5.8.

Affected Software/OS:

Pidgin version prior to 2.5.8 on Linux

References:

<http://secunia.com/advisories/35652>

<http://developer.pidgin.im/ticket/9483>

<http://pidgin.im/pipermail/devel/2009-May/008227.html>

CVSS Base Score: 5.0

Family name: Denial of Service

Category: infos

Copyright: Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12670 \$

CVEs: CVE-2009-1889

Medium:

Pidgin Oscar Protocol Denial of Service Vulnerability (Linux)

Risk: Medium

Application: general

Port: 0

Protocol: tcp

ScriptID: 801031

Vulnerability Detection Result:

Installed version: 2.5.2

Fixed version: 2.6.3

Affected Software/OS:

Pidgin version prior to 2.6.3 on Linux.

Solution:

Upgrade to Pidgin version 2.6.3.

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.

Impact:

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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:P

Summary:

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

References:

<http://secunia.com/advisories/37072>

<http://xforce.iss.net/xforce/xfdb/53807>

<http://www.pidgin.im/news/security/?id=41>

<http://developer.pidgin.im/wiki/ChangeLog>

CVSS Base Score: 5.0

Family name: Denial of Service

Category: infos

Copyright: Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 12670 \$

CVEs: CVE-2009-3615

Low:

### SSH Weak MAC Algorithms Supported

Risk: Low

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 105610

Vulnerability Detection Result:

The following weak client-to-server MAC algorithms are supported by the remote service:

hmac-md5

hmac-md5-96

hmac-sha1-96

The following weak server-to-client MAC algorithms are supported by the remote service:

hmac-md5

hmac-md5-96

hmac-sha1-96

Summary:

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

CVSS Base Vector:

AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution:

Disable the weak MAC algorithms.

CVSS Base Score: 2.6

Family name: General

Category: infos

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-26T13:48:10+0000

Low:

TCP timestamps

Risk: Low

Application: general

Port: 0

Protocol: tcp

ScriptID: 80091

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: 569429

Packet 2: 569531

Impact:

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

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.

CVSS Base Vector:

AV:N/AC:H/Au:N/C:P/I:N/A:N

Summary:

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

Insight:

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

Solution:

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.

See the references for more information.

Affected Software/OS:

TCP/IPv4 implementations that implement RFC1323.

References:

<http://www.ietf.org/rfc/rfc1323.txt>

<http://www.microsoft.com/en-us/download/details.aspx?id=9152>

CVSS Base Score: 2.6

Family name: General

Category: unknown

Copyright: Copyright (C) 2008 Michel Arboi

Version: 2020-03-21T13:23:23+0000

Low:

Ubuntu Update for apache2 USN-1627-1

Risk: Low

Application: general

Port: 0

Protocol: tcp

ScriptID: 841209

Vulnerability Detection Result:

Vulnerable package: apache2.2-common

Installed version: 2.2.8-1ubuntu0.15

Fixed version: 2.2.8-1ubuntu0.24

Affected Software/OS:

apache2 on Ubuntu 12.10,

Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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)

CVSS Base Vector:

AV:N/AC:H/Au:N/C:N/I:P/A:N

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1627-1

References:

<http://www.ubuntu.com/usn/usn-1627-1/>

USN:1627-1

[http://httpd.apache.org/docs/2.4/mod/mod\\_ssl.html](http://httpd.apache.org/docs/2.4/mod/mod_ssl.html)

CVSS Base Score: 2.6

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-2687, CVE-2012-4929

Low:

Ubuntu Update for apt USN-1283-1

Risk: Low

Application: general

Port: 0

Protocol: tcp

ScriptID: 840825

Vulnerability Detection Result:

Vulnerable package: apt

Installed version: 0.7.9ubuntu17

Fixed version: 0.7.9ubuntu17.4

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)

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.

Affected Software/OS:

apt on Ubuntu 11.04,

Ubuntu 10.10,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:N/AC:H/Au:N/C:P/I:N/A:N

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1283-1

References:

<http://www.ubuntu.com/usn/usn-1283-1/>

USN:1283-1

CVSS Base Score: 2.6

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2011-3634

Low:

Ubuntu Update for apt USN-1475-1

Risk: Low

Application: general

Port: 0

Protocol: tcp

ScriptID: 841037

Vulnerability Detection Result:

Vulnerable package: apt

Installed version: 0.7.9ubuntu17

Fixed version: 0.7.9ubuntu17.5

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.

Solution:

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

CVSS Base Vector:

AV:N/AC:H/Au:N/C:N/I:P/A:N

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1475-1

References:

<http://www.ubuntu.com/usn/usn-1475-1/>

USN:1475-1

CVSS Base Score: 2.6

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-0954, CVE-2012-3587

Low:

Ubuntu Update for apt USN-1477-1

Risk: Low

Application: general

Port: 0

Protocol: tcp

ScriptID: 841045

Vulnerability Detection Result:

Vulnerable package: apt

Installed version: 0.7.9ubuntu17

Fixed version: 0.7.9ubuntu17.6

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1477-1

CVSS Base Vector:

AV:N/AC:H/Au:N/C:N/I:P/A:N

Affected Software/OS:

apt on Ubuntu 12.04 LTS,

Ubuntu 11.10,

Ubuntu 11.04,

Ubuntu 10.04 LTS,

Ubuntu 8.04 LTS

Solution:

Please Install the Updated Packages.

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.

References:

<http://www.ubuntu.com/usn/usn-1477-1/>

USN:1477-1

CVSS Base Score: 2.6

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2012-0954



Low:

Ubuntu Update for dbus vulnerability USN-1044-1

Risk: Low

Application: general

Port: 0

Protocol: tcp

ScriptID: 840570

Vulnerability Detection Result:

Vulnerable package: libdbus-1-3

Installed version: 1.1.20-1ubuntu1

Fixed version: 1.1.20-1ubuntu3.4

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.

Solution:

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

CVSS Base Vector:

AV:L/AC:L/Au:N/C:N/I:N/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1044-1

References:

<http://www.ubuntu.com/usn/usn-1044-1/>

USN:1044-1

CVSS Base Score: 2.1

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2010-4352

Low:

Ubuntu Update for fuse vulnerabilities USN-1077-1

Risk: Low

Application: general

Port: 0

Protocol: tcp

ScriptID: 840606

Vulnerability Detection Result:

Vulnerable package: fuse-utils

Installed version: 2.7.2-1ubuntu2

Fixed version: 2.7.2-1ubuntu2.3

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.

Affected Software/OS:

fuse vulnerabilities on Ubuntu 8.04 LTS,

Ubuntu 9.10,

Ubuntu 10.04 LTS,

Ubuntu 10.10

Solution:

Please Install the Updated Packages.

CVSS Base Vector:

AV:L/AC:M/Au:N/C:N/I:P/A:P

Summary:

Ubuntu Update for Linux kernel vulnerabilities USN-1077-1

References:

<http://www.ubuntu.com/usn/usn-1077-1/>

USN:1077-1

CVSS Base Score: 3.3

Family name: Ubuntu Local Security Checks

Category: infos

Copyright: Copyright (c) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 14132 \$

CVEs: CVE-2009-3297, CVE-2011-0541, CVE-2011-0542, CVE-2011-0543

Low:

## ICMP Timestamp Detection

Risk: Low

Application: general

Port: 0

Protocol: icmp

ScriptID: 103190

Summary:

The remote host responded to an ICMP timestamp request.

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

CVSS Base Vector:

AV:L/AC:L/Au:N/C:N/I:N/A:N

References:

<http://www.ietf.org/rfc/rfc0792.txt>

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 10411 \$

CVEs: CVE-1999-0524

## Info:

7zip Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 800255

Vulnerability Detection Result:

Detected 7zip version: 4.57

Location: /usr/bin/7za

CPE: cpe:/a:7-zip:7-zip:4.57

Concluded from version identification result:

7-Zip (A) 4.57 Copyright (c) 1999-2007 Igor Pavlov 2007-12-06

p7zip Version 4.57 (locale=C,Utf16=off,HugeFiles=on,1 CPU)

## Error:

Incorrect command line

Summary:

Detects the installed version of 7zip.

The script logs in via ssh, searches for executable '7za' and queries the found executables via command line option 'invalidcmd'.

The error message output of 7za is normal because 7za in fact offers no version command and thus an invalid command has to be passed to obtain the version number.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

rsh Service Detection

Risk: Info

Application: shell

Port: 514

Protocol: tcp

ScriptID: 108478

Vulnerability Detection Result:

A rsh service is running at this port.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Checks if the remote host is running a rsh service.

Note: The reporting takes place in a separate VT 'rsh Unencrypted Cleartext Login' (OID: 1.3.6.1.4.1.25623.1.0.100080).

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-09-17T06:05:09+0000

Info:

Ruby Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 900569

Vulnerability Detection Result:

Detected Ruby version: 1.8.6.p111

Location: /usr/bin/ruby

CPE: cpe:/a:ruby-lang:ruby:1.8.6.p111:p111

Concluded from version identification result:

ruby 1.8.6 (2007-09-24 patchlevel 111) [i486-linux]

Summary:

Detects the installed version of Ruby.

The script logs in via ssh, searches for executable 'ruby' and queries the found executables via command line option '--version'.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

Samba Version Detection

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 800403

Vulnerability Detection Result:

Detected Samba

Version: 3.0.20-Debian

Location: /usr/sbin/smbd

CPE: cpe:/a:samba:samba:3.0.20

Concluded from version/product identification result:

3.0.20-Debian

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detects the installed version of Samba.

The script logs in via SSH, searches for executable 'smbd' and queries the found executables via command line option '-V'.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

Service Detection with 'BINARY' Request

Risk: Info

Application: login

Port: 513

Protocol: tcp

ScriptID: 108204

Vulnerability Detection Result:

A rlogin service seems to be running on this port.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This plugin performs service detection.

This plugin is a complement of find\_service.nasl. It sends a 'BINARY' request to the remaining unknown services and tries to identify them.

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: Copyright (c) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-02-20T07:23:20+0000

Info:

Service Detection with 'BINARY' Request

Risk: Info

Application: exec

Port: 512

Protocol: tcp

ScriptID: 108204

Vulnerability Detection Result:

A rexec service seems to be running on this port.

Summary:

This plugin performs service detection.

This plugin is a complement of find\_service.nasl. It sends a 'BINARY' request to the remaining unknown services and tries to identify them.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: Copyright (c) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-02-20T07:23:20+0000

Info:

Service Detection with 'GET' Request

Risk: Info

Application: unknown

Port: 8787

Protocol: tcp

ScriptID: 17975

Vulnerability Detection Result:

A Distributed Ruby (dRuby/DRb) service seems to be running on this port.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This plugin performs service detection.

This plugin is a complement of find\_service.nasl. It sends a 'GET' request to the remaining unknown services and tries to identify them.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2005 Michel Arboi

Version: 2020-03-25T13:50:09+0000

Info:

Service Detection with 'GET' Request

Risk: Info

Application: irc

Port: 6667

Protocol: tcp

ScriptID: 17975

Vulnerability Detection Result:

An IRC server seems to be running on this port.

Summary:

This plugin performs service detection.

This plugin is a complement of find\_service.nasl. It sends a 'GET' request to the remaining unknown services and tries to identify them.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2005 Michel Arboi

Version: 2020-03-25T13:50:09+0000

Info:

Service Detection with 'GET' Request

Risk: Info

Application: ingreslock

Port: 1524

Protocol: tcp

ScriptID: 17975

Vulnerability Detection Result:

A root shell of Metasploitable seems to be running on this port.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This plugin performs service detection.

This plugin is a complement of find\_service.nasl. It sends a 'GET' request to the remaining unknown services and tries to identify them.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2005 Michel Arboi

Version: 2020-03-25T13:50:09+0000



Info:

Services

Risk: Info

Application: unknown

Port: 2121

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

An FTP server is running on this port.

Here is its banner :

220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.56.12]

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A web server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: smtp

Port: 25

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

An SMTP server is running on this port

Here is its banner :

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

An ssh server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

An FTP server is running on this port.

Here is its banner :

220 (vsFTPd 2.3.4)

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: postgres

Port: 5432

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

An unknown service is running on this port.

It is usually reserved for Postgres

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: telnet

Port: 23

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

A telnet server seems to be running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

Services

Risk: Info

Application: mysql

Port: 3306

Protocol: tcp

ScriptID: 10330

Vulnerability Detection Result:

An unknown service is running on this port.

It is usually reserved for MySQL

Summary:

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>

Version: 2019-07-08T14:12:44+0000

Info:

SMB log in

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 10394

Vulnerability Detection Result:

It was possible to log into the remote host using the SMB protocol.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

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

CVSS Base Score: 0.0

Family name: Windows

Category: unknown

Copyright: Copyright (C) 2008 SecPod

Version: 2019-10-16T06:21:07+0000

Info:

SMB Login Successful For Authenticated Checks

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 108539

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

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

CVSS Base Score: 0.0

Family name: Windows

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: \$Revision: 13248 \$

Info:

SMB NativeLanMan

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 102011

Vulnerability Detection Result:

Detected Samba

Version: 3.0.20

Location: 445/tcp

CPE: cpe:/a:samba:samba:3.0.20

Concluded from version/product identification result:

Samba 3.0.20-Debian

Extra information:

Detected SMB workgroup: WORKGROUP

Detected SMB server: Samba 3.0.20-Debian

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

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

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: Copyright (C) 2009 LSS

Summary: NOSUMMARY

Version: 2019-12-12T09:38:57+0000

Info:

SMB NativeLanMan

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 102011

Vulnerability Detection Result:

Detected SMB workgroup: WORKGROUP

Detected SMB server: Samba 3.0.20-Debian

Detected OS: Debian GNU/Linux

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

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

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: Copyright (C) 2009 LSS

Summary: NOSUMMARY

Version: 2019-12-12T09:38:57+0000

Info:

SMB Remote Version Detection

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 807830

Vulnerability Detection Result:

Only SMBv1 is enabled on remote target

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detection of Server Message Block(SMB).

This script sends SMB Negotiation request and try to get the version from the response.

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-05-16T07:13:31+0000

Info:

SMB/CIFS Server Detection

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 11011

Vulnerability Detection Result:

A CIFS server is running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: This script is Copyright (C) 2002 Renaud Deraison

Version: \$Revision: 13541 \$

Info:

SMB/CIFS Server Detection

Risk: Info

Application: netbios-ssn

Port: 139

Protocol: tcp

ScriptID: 11011

Vulnerability Detection Result:

A SMB server is running on this port

Summary:

This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: This script is Copyright (C) 2002 Renaud Deraison

Version: \$Revision: 13541 \$

Info:

SMBv1 enabled (Remote Check)

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 140151

Vulnerability Detection Result:

SMBv1 is enabled for the SMB Server

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

The host has enabled SMBv1 for the SMB Server.

Vulnerability Detection Method:

Checks if SMBv1 is enabled for the SMB Server based on the information provided by the following VT:

- SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830).

References:

<https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices>

<https://support.microsoft.com/en-us/kb/2696547>

<https://support.microsoft.com/en-us/kb/204279>

CVSS Base Score: 0.0

Family name: Windows

Category: infos

Copyright: Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-05-20T06:24:13+0000



Info:

SMTP Server type and version

Risk: Info

Application: smtp

Port: 25

Protocol: tcp

ScriptID: 10263

Vulnerability Detection Result:

Remote SMTP server banner:

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

The remote SMTP server is announcing the following available ESMTP commands (EHLO response) via an unencrypted connection:

8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, STARTTLS, VRFY

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This detects the SMTP Server's type and version by connecting to the server and processing the buffer received.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2005 SecuriTeam

Version: 2020-03-27T07:53:12+0000

Info:

SSH Authorization Check

Risk: Info

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 90022

Vulnerability Detection Result:

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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script tries to login with provided credentials.

If the login was successful, it marks this port as available for any authenticated tests.

CVSS Base Score: 0.0

Family name: General

Category: unknown

Copyright: Copyright 2007-2012 Greenbone Networks GmbH

Version: 2019-12-17T14:36:50+0000

Info:

SSH Login Successful For Authenticated Checks

Risk: Info

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 108540

Summary:

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

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: General

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: \$Revision: 13248 \$

Info:

SSH Protocol Algorithms Supported

Risk: Info

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 105565

Vulnerability Detection Result:

The following options are supported by the remote ssh service:

kex\_algorithms:

diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

server\_host\_key\_algorithms:

ssh-rsa,ssh-dss

encryption\_algorithms\_client\_to\_server:

aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr

encryption\_algorithms\_server\_to\_client:

aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr

mac\_algorithms\_client\_to\_server:

hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96

mac\_algorithms\_server\_to\_client:

hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96

compression\_algorithms\_client\_to\_server:

none,zlib@openssh.com

compression\_algorithms\_server\_to\_client:

none,zlib@openssh.com

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script detects which algorithms are supported by the remote SSH Service.

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-26T13:48:10+0000

Info:

SSH Protocol Versions Supported

Risk: Info

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 100259

Vulnerability Detection Result:

The remote SSH Server supports the following SSH Protocol Versions:

1.99

2.0

SSHv2 Fingerprint(s):

ssh-dss: 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd

ssh-rsa: 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.

The following versions are tried: 1.33, 1.5, 1.99 and 2.0

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-26T13:48:10+0000

Info:

SSH Server type and version

Risk: Info

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 10267

Vulnerability Detection Result:

Remote SSH server banner: SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu1

Remote SSH supported authentication: password,publickey

Remote SSH text/login banner: (not available)

This is probably:

- OpenSSH

Concluded from remote connection attempt with credentials:

Login: msfadmin

Password: SSH password/private key configured for this task

Summary:

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking.

Versions and Types should be omitted where possible.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2006 SecuriTeam

Version: 2020-03-26T13:48:10+0000

Info:

SSL/TLS: Certificate - Self-Signed Certificate Detection

Risk: Info

Application: smtp

Port: 25

Protocol: tcp

ScriptID: 103140

Vulnerability Detection Result:

The certificate of the remote service is self signed.

Certificate details:

subject ...:

1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX

subject alternative names (SAN):

None

issued by .:

1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside 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): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436DE813CC

Summary:

The SSL/TLS certificate on this port is self-signed.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

[http://en.wikipedia.org/wiki/Self-signed\\_certificate](http://en.wikipedia.org/wiki/Self-signed_certificate)

CVSS Base Score: 0.0

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 8981 \$

Info:

SSL/TLS: Certificate - Self-Signed Certificate Detection

Risk: Info

Application: postgres

Port: 5432

Protocol: tcp

ScriptID: 103140

Vulnerability Detection Result:

The certificate of the remote service is self signed.

Certificate details:

subject ...:

1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX

subject alternative names (SAN):

None

issued by .:

1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside 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): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436DE813CC

Summary:

The SSL/TLS certificate on this port is self-signed.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

[http://en.wikipedia.org/wiki/Self-signed\\_certificate](http://en.wikipedia.org/wiki/Self-signed_certificate)

CVSS Base Score: 0.0

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 8981 \$

Info:

SSL/TLS: Collect and Report Certificate Details

Risk: Info

Application: smtp

Port: 25

Protocol: tcp

ScriptID: 103692

Vulnerability Detection Result:

The following certificate details of the remote service were collected.

Certificate details:

subject ...:

1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX

subject alternative names (SAN):

None

issued by .:

1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside 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): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436DE813CC

Summary:

This script collects and reports the details of all SSL/TLS certificates.

This data will be used by other tests to verify server certificates.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: SSL and TLS

Category: infos

Copyright: Copyright 2013 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-04-04T13:38:03+0000



Info:

SSL/TLS: Collect and Report Certificate Details

Risk: Info

Application: postgres

Port: 5432

Protocol: tcp

ScriptID: 103692

Vulnerability Detection Result:

The following certificate details of the remote service were collected.

Certificate details:

subject ...:

1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX

subject alternative names (SAN):

None

issued by .:

1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside 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): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436DE813CC

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script collects and reports the details of all SSL/TLS certificates.

This data will be used by other tests to verify server certificates.

CVSS Base Score: 0.0

Family name: SSL and TLS

Category: infos

Copyright: Copyright 2013 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-04-04T13:38:03+0000

Info:

SSL/TLS: Hostname discovery from server certificate

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 111010

Vulnerability Detection Result:

The following additional but not resolvable hostnames were detected:

ubuntu804-base.localdomain

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

It was possible to discover an additional hostname  
of this server from its certificate Common or Subject Alt Name.

CVSS Base Score: 0.0

Family name: SSL and TLS

Category: infos

Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH

Summary: NOSUMMARY

Version: \$Revision: 13774 \$

Info:

PostgreSQL TLS Detection

Risk: Info

Application: postgres

Port: 5432

Protocol: tcp

ScriptID: 105013

Vulnerability Detection Result:

The remote PostgreSQL server supports SSL/TLS.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Checks if the remote PostgreSQL server supports SSL/TLS.

References:

<https://www.postgresql.org/docs/current/static/ssl-tcp.html>

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: This script is Copyright (C) 2014 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-01-28T13:26:39+0000

Info:

SMTP STARTTLS Detection

Risk: Info

Application: smtp

Port: 25

Protocol: tcp

ScriptID: 103118

Vulnerability Detection Result:

The remote SMTP server supports SSL/TLS with the 'STARTTLS' command.

The remote SMTP server is announcing the following available ESMTP commands (EHLO response) before sending the 'STARTTLS' command:

8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, STARTTLS, VRFY

The remote SMTP server is announcing the following available ESMTP commands (EHLO response) after sending the 'STARTTLS' command:

8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, VRFY

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Checks if the remote SMTP server supports SSL/TLS with the 'STARTTLS' command.

References:

<https://tools.ietf.org/html/rfc3207>

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-23T13:51:29+0000

## Info:

### CPE Inventory

Risk: Info

Application: general

Port: 0

Protocol: CPE-T

ScriptID: 810002

### Vulnerability Detection Result:

192.168.56.12|cpe:/a:7-zip:7-zip:4.57  
192.168.56.12|cpe:/a:andy\_armstrong:cgi.pm:3.15  
192.168.56.12|cpe:/a:apache:http\_server:2.2.8  
192.168.56.12|cpe:/a:beasts:vsftpd:2.3.4  
192.168.56.12|cpe:/a:gnu:assembler:2.18.0  
192.168.56.12|cpe:/a:gnu:bash:3.2.33  
192.168.56.12|cpe:/a:gnu:binutils:2.18.0.20080103  
192.168.56.12|cpe:/a:gnu:gcc:4.2.4  
192.168.56.12|cpe:/a:gnu:gzip:1.2.4  
192.168.56.12|cpe:/a:gnu:gzip:1.3.12  
192.168.56.12|cpe:/a:isc:bind:9.4.2  
192.168.56.12|cpe:/a:jquery:jquery  
192.168.56.12|cpe:/a:mit:kerberos:1.6.3  
192.168.56.12|cpe:/a:mozilla:firefox:3.6.17  
192.168.56.12|cpe:/a:mysql:mysql:5.0.51a  
192.168.56.12|cpe:/a:openbsd:openssh:4.7p1  
192.168.56.12|cpe:/a:openssl:openssl:0.9.8g  
192.168.56.12|cpe:/a:perl:perl:5.8.8  
192.168.56.12|cpe:/a:php:php:5.2.4  
192.168.56.12|cpe:/a:phpmyadmin:phpmyadmin:3.1.1  
192.168.56.12|cpe:/a:pidgin:pidgin:2.5.2  
192.168.56.12|cpe:/a:postfix:postfix  
192.168.56.12|cpe:/a:postgresql:postgresql:8.3.1  
192.168.56.12|cpe:/a:proftpd:proftpd:1.3.1  
192.168.56.12|cpe:/a:python:python:2.5.2  
192.168.56.12|cpe:/a:rafael\_garcia-suarez:safe:2.29  
192.168.56.12|cpe:/a:ruby-lang:ruby:1.8.6.p111:p111  
192.168.56.12|cpe:/a:samba:samba:3.0.20  
192.168.56.12|cpe:/a:tcpdump:libpcap:0.9.8  
192.168.56.12|cpe:/a:tcpdump:tcpdump:3.9.8  
192.168.56.12|cpe:/a:twiki:twiki:01.Feb.2003  
192.168.56.12|cpe:/a:unrealircd:unrealircd:3.2.8.1  
192.168.56.12|cpe:/a:x.org:x11:11.0  
192.168.56.12|cpe:/o:canonical:ubuntu\_linux:8.04:-:lts

### Summary:

This routine uses information collected by other routines about

CPE identities of operating systems, services and applications detected during the scan.

Note: Some CPEs for specific products might show up twice or more in the output. Background:

After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.

### CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

### References:

<https://nvd.nist.gov/products/cpe>

CVSS Base Score: 0.0

Family name: Service detection

Category: end

Copyright: Copyright (c) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-10-24T11:29:24+0000

Info:

tcpdump Detection (SSH)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 113542

Vulnerability Detection Result:

Detected tcpdump

Version: 3.9.8

Location: /usr/sbin/tcpdump

CPE: cpe:/a:tcpdump:tcpdump:3.9.8

Concluded from version/product identification result:

tcpdump version 3.9.8

Summary:

Checks whether tcpdump is installed on the target system  
and if so, tries to detect the installed version.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

<https://www.tcpdump.org/>

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: 2020-03-27T14:05:33+0000

Info:

tcpdump Detection (SSH)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 113542

Vulnerability Detection Result:

Detected libpcap

Version: 0.9.8

Location: /usr/sbin/tcpdump

CPE: cpe:/a:tcpdump:libpcap:0.9.8

Concluded from version/product identification result:

libpcap version 0.9.8

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Checks whether tcpdump is installed on the target system  
and if so, tries to detect the installed version.

References:

<https://www.tcpdump.org/>

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: 2020-03-27T14:05:33+0000

Info:

## Telnet Banner Reporting

### Risk: Info

Application: telnet

Port: 23

Protocol: tcp

ScriptID: 10281

### Vulnerability Detection Result:

Remote Telnet banner:

一 二 三 四 五 六 七 八 九 十 十一 十二 十三 十四 十五 十六 十七 十八 十九 二十 二十一 二十二 二十三 二十四 二十五 二十六 二十七 二十八 二十九 三十 三十一 三十二 三十三 三十四 三十五 三十六 三十七 三十八 三十九 四十 四十一 四十二 四十三 四十四 四十五 四十六 四十七 四十八 四十九 五十 五十一 五十二 五十三 五十四 五十五 五十六 五十七 五十八 五十九 六十 六十一 六十二 六十三 六十四 六十五 六十六 六十七 六十八 六十九 七十 七十一 七十二 七十三 七十四 七十五 七十六 七十七 七十八 七十九 八十 八十一 八十二 八十三 八十四 八十五 八十六 八十七 八十八 八十九 九十 九十一 九十二 九十三 九十四 九十五 九十六 九十七 九十八 九十九 一百

Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

metasploitable login:

Summary:

This scripts reports the received banner of a Telnet service.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2005 SecuriTeam

Version: 2020-03-20T10:26:01+0000



Info:

Check for Telnet Server

Risk: Info

Application: telnet

Port: 23

Protocol: tcp

ScriptID: 100074

Vulnerability Detection Result:

A Telnet server seems to be running on this port

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This scripts tries to detect a Telnet service running  
at the remote host.

References:

<https://tools.ietf.org/html/rfc854>

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-21T13:23:23+0000

Info:

Traceroute

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 51662

Vulnerability Detection Result:

Here is the route from 192.168.56.11 to 192.168.56.12:

192.168.56.11

192.168.56.12

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

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

Solution:

Block unwanted packets from escaping your network.

CVSS Base Score: 0.0

Family name: General

Category: unknown

Copyright: Copyright (C) 2010 E-Soft Inc. <http://www.securityspace.com>

Version: 2020-03-21T13:23:23+0000

Info:

Database Open Access Vulnerability

Risk: Info

Application: postgres

Port: 5432

Protocol: tcp

ScriptID: 902799

Vulnerability Detection Result:

PostgreSQL database can be accessed by remote attackers

Insight:

Do not restricting direct access of databases to the remote systems.

Affected Software/OS:

- MySQL/MariaDB
  - IBM DB2
  - PostgreSQL
  - IBM solidDB
  - Oracle Database
  - Microsoft SQL Server

Solution:

Restrict Database access to remote systems.

Impact:

Successful exploitation could allow an attacker to obtain the sensitive information of the database.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

The host is running a Database server and is prone to information disclosure vulnerability.

References:

[https://www.pcisecuritystandards.org/security\\_standards/index.php?id=pci\\_dss\\_v1-2.pdf](https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf)

CVSS Base Score: 0.0

Family name: Databases

Category: infos

Copyright: Copyright (C) 2012 SecPod

Summary: NOSUMMARY

Version: 2020-03-21T13:23:23+0000

Info:

TWiki Version Detection

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 800399

Vulnerability Detection Result:

Detected TWiki

Version: 01.Feb.2003

Location: /twiki/bin

CPE: cpe:/a:twiki:twiki:01.Feb.2003

Concluded from version/product identification result:

This site is running TWiki version <strong>01 Feb 2003</strong>

Summary:

Detection of TWiki.

The script sends a HTTP connection request to the server and attempts to detect the presence of TWiki and to extract its version.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-12-04T13:23:25+0000

## Info:

### Database Open Access Vulnerability

Risk: Info

Application: mysql

Port: 3306

Protocol: tcp

ScriptID: 902799

Vulnerability Detection Result:

MySQL can be accessed by remote attackers

Solution:

Restrict Database access to remote systems.

Affected Software/OS:

- MySQL/MariaDB
  - IBM DB2
  - PostgreSQL
  - IBM solidDB
  - Oracle Database
  - Microsoft SQL Server

Insight:

Do not restricting direct access of databases to the remote systems.

Impact:

Successful exploitation could allow an attacker to obtain the sensitive information of the database.

Summary:

The host is running a Database server and is prone to information disclosure vulnerability.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

[https://www.pcisecuritystandards.org/security\\_standards/index.php?id=pci\\_dss\\_v1-2.pdf](https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf)

CVSS Base Score: 0.0

Family name: Databases

Category: infos

Copyright: Copyright (C) 2012 SecPod

Summary: NOSUMMARY

Version: 2020-03-21T13:23:23+0000

Info:

Determine OS and list of installed packages via SSH login

Risk: Info

Application: ssh

Port: 22

Protocol: tcp

ScriptID: 50282

Vulnerability Detection Result:

We are able to login and detect that you are running Ubuntu 8.04 LTS.

Summary:

This script will, if given a userid/password or

key to the remote system, login to that system, determine the OS it is running, and for supported systems, extract the list of installed packages/rpms.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Insight:

The ssh protocol is used to log in. If a specific port is

configured for the credential, then only this port will be tried. Else any port that offers ssh, usually port 22.

Upon successful login, the command 'uname -a' is issued to find out about the type and version of the operating system.

The result is analysed for various patterns and in several cases additional commands are tried to find out more details and to confirm a detection.

The regular Linux distributions are detected this way as well as other unixoid systems and also many Linux-based devices and appliances.

If the system offers a package database, for example RPM- or DEB-based, this full list of installed packages is retrieved for further patch-level checks.

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2008 E-Soft Inc. <http://www.securityspace.com> & Tim Brown

Version: 2020-03-26T09:43:37+0000

Info:

DistCC Detection

Risk: Info

Application: unknown

Port: 3632

Protocol: tcp

ScriptID: 12638

Vulnerability Detection Result:

A DistCC service is running at this port.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Tries to detect if the remote host is running a DistCC service.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: This script is Copyright (C) 2005 Noam Rathaus

Version: \$Revision: 13541 \$

Info:

7zip Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 800255

Vulnerability Detection Result:

Detected 7zip version: 4.57

Location: /usr/lib/p7zip/7za

CPE: cpe:/a:7-zip:7-zip:4.57

Concluded from version identification result:

7-Zip (A) 4.57 Copyright (c) 1999-2007 Igor Pavlov 2007-12-06

p7zip Version 4.57 (locale=C,Utf16=off,HugeFiles=on,1 CPU)

Error:

Incorrect command line

Summary:

Detects the installed version of 7zip.

The script logs in via ssh, searches for executable '7za' and queries the found executables via command line option 'invalidcmd'.

The error message output of 7za is normal because 7za in fact offers no version command and thus an invalid command has to be passed to obtain the version number.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

DNS Server Detection (TCP)

Risk: Info

Application: domain

Port: 53

Protocol: tcp

ScriptID: 108018

Vulnerability Detection Result:

The remote DNS server banner is:  
9.4.2

Summary:

A DNS Server is running at this Host.

A Name Server translates domain names into IP addresses. This makes it possible for a user to access a website by typing in the domain name instead of the website's actual IP address.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 13541 \$

Info:

Fingerprint web server with favicon.ico

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 20108

Vulnerability Detection Result:

The following apps/services were identified:

"phpmyadmin (2.11.8.1 - 4.2.x)" fingerprinted by the file: "http://192.168.56.12/phpMyAdmin/favicon.ico"

Solution:

Remove the 'favicon.ico' file or create a custom one for your site.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

The remote web server contains a graphic image that is prone to information disclosure.

Impact:

The 'favicon.ico' file found on the remote web server belongs to a popular webserver/application. This may be used to fingerprint the webserver/application.

CVSS Base Score: 0.0

Family name: Web application abuses

Category: unknown

Copyright: Copyright (C) 2005 Javier Fernandez-Sanguino

Version: 2020-02-26T12:57:19+0000

Info:

FTP Banner Detection

Risk: Info

Application: unknown

Port: 2121

Protocol: tcp

ScriptID: 10092

Vulnerability Detection Result:

Remote FTP server banner:

220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.56.12]

This is probably:

- ProFTPD

Server operating system information collected via "SYST" command:

215 UNIX Type: L8

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This Plugin detects and reports a FTP Server Banner.

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2005 SecuriTeam

Version: 2020-03-24T12:27:11+0000



Info:

FTP Banner Detection

Risk: Info

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 10092

Vulnerability Detection Result:

Remote FTP server banner:

220 (vsFTPd 2.3.4)

This is probably:

- vsFTPd

Server operating system information collected via "SYST" command:

215 UNIX Type: L8

Server status information collected via "STAT" command:

211-FTP server status:

Connected to 192.168.56.11

Logged in as ftp

TYPE: ASCII

No session bandwidth limit

Session timeout in seconds is 300

Control connection is plain text

Data connections will be plain text

vsFTPd 2.3.4 - secure, fast, stable

211 End of status

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This Plugin detects and reports a FTP Server Banner.

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2005 SecuriTeam

Version: 2020-03-24T12:27:11+0000

Info:

UnrealIRCd Detection

Risk: Info

Application: irc

Port: 6667

Protocol: tcp

ScriptID: 809884

Vulnerability Detection Result:

Detected UnrealIRCd

Version: 3.2.8.1

Location: 6667/tcp

CPE: cpe:/a:unrealircd:unrealircd:3.2.8.1

Concluded from version/product identification result:

Unreal3.2.8.1

Summary:

Detection of UnrealIRCd Daemon. This script

sends a request to the server and gets the version from the response.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 10987 \$

Info:

VNC security types

Risk: Info

Application: vnc

Port: 5900

Protocol: tcp

ScriptID: 19288

Vulnerability Detection Result:

The remote VNC server chose security type #2 (VNC authentication)

Summary:

This script checks the remote VNC protocol version

and the available 'security types'.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: This script is Copyright (C) 2006 Michel Arboi

Version: \$Revision: 13541 \$

Info:

VNC Server and Protocol Version Detection

Risk: Info

Application: vnc

Port: 5900

Protocol: tcp

ScriptID: 10342

Vulnerability Detection Result:

A VNC server seems to be running on this port.

The version of the VNC protocol is : RFB 003.003

Summary:

The remote host is running a remote display software (VNC) which permits a console to be displayed remotely.

This allows authenticated users of the remote host to take its control remotely.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution:

Make sure the use of this software is done in accordance with your corporate security policy, filter incoming traffic to this port.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: This script is Copyright (C) 2000 Patrick Naubert

Version: \$Revision: 13541 \$

Info:

vsFTPD FTP Server Detection

Risk: Info

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 111050

Vulnerability Detection Result:

Detected vsFTPD

Version: 2.3.4

Location: 21/tcp

CPE: cpe:/a:beasts:vsftpd:2.3.4

Concluded from version/product identification result:

220 (vsFTPD 2.3.4)

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

The script is grabbing the banner of a FTP server and attempts to identify a vsFTPD FTP Server and its version from the reply.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH

Summary: NOSUMMARY

Version: 2020-03-24T12:27:11+0000

## Info:

### X Server Detection

Risk: Info

Application: X11

Port: 6000

Protocol: tcp

ScriptID: 10407

Vulnerability Detection Result:

Detected X Windows Server

Version: 11.0

Location: 6000/tcp

CPE: cpe:/a:x.org:x11:11.0

Concluded from version/product identification result:

11.0

Extra information:

Server answered with: Client is not authorized

Summary:

This plugin detects X Window servers.

X11 is a client - server protocol. Basically, the server is in charge of the screen, and the clients connect to it and send several requests like drawing a window or a menu, and the server sends events back to the clients, such as mouse clicks, key strokes, and so on...

An improperly configured X server will accept connections from clients from anywhere. This allows an attacker to make a client connect to the X server to record the keystrokes of the user, which may contain sensitive information, such as account passwords.

This can be prevented by using xauth, MIT cookies, or preventing the X server from listening on TCP (a Unix sock is used for local connections)

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: This script is Copyright (C) 2000 John Jackson

Version: \$Revision: 10123 \$

Info:

FTP Missing Support For AUTH TLS

Risk: Info

Application: unknown

Port: 2121

Protocol: tcp

ScriptID: 108553

Vulnerability Detection Result:

The remote FTP server does not support the 'AUTH TLS' command.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

The remote FTP server does not support the 'AUTH TLS' command.

CVSS Base Score: 0.0

Family name: FTP

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: \$Revision: 13863 \$

Info:

FTP Missing Support For AUTH TLS

Risk: Info

Application: ftp

Port: 21

Protocol: tcp

ScriptID: 108553

Vulnerability Detection Result:

The remote FTP server does not support the 'AUTH TLS' command.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

The remote FTP server does not support the 'AUTH TLS' command.

CVSS Base Score: 0.0

Family name: FTP

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: \$Revision: 13863 \$

Info:

GNU\_Assembler Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 806084

Vulnerability Detection Result:

Detected GNU Assembler

Version: 2.18.0

Location: /usr/bin/as

CPE: cpe:/a:gnu:assembler:2.18.0

Concluded from version/product identification result:

GNU assembler version 2.18.0 (i486-linux-gnu) using BFD version (GNU Binutils for Ubuntu) 2.18.0.20080103

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detects the installed version of GNU Assembler.

The script logs in via ssh, searches for executable 'as' and queries the found executables via command line option '-v'

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2015 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

GCC Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 108258

Vulnerability Detection Result:

Detected GNU bash

Version: 3.2.33

Location: /bin/bash

CPE: cpe:/a:gnu:bash:3.2.33

Concluded from version/product identification result:

GNU bash, version 3.2.33

Summary:

Detects the installed version of GNU bash.

The script logs in via SSH, searches for the executable 'bash' and queries the found executables via the command line option '--version'

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

GNU Binutils Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 806085

Vulnerability Detection Result:

Detected GNU Binutils

Version: 2.18.0.20080103

Location: /usr/bin/as

CPE: cpe:/a:gnu:binutils:2.18.0.20080103

Concluded from version/product identification result:

GNU assembler version 2.18.0 (i486-linux-gnu) using BFD version (GNU Binutils for Ubuntu) 2.18.0.20080103

Summary:

Detects the installed version of GNU Binutils.

The script tries to enumerate the installed Binutils version(s) from various previously found binaries included in this suite.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2015 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-12-09T15:47:13+0000



Info:

GCC Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 806083

Vulnerability Detection Result:

Detected GNU GCC

Version: 4.2.4

Location: /usr/bin/gcc

CPE: cpe:/a:gnu:gcc:4.2.4

Concluded from version/product identification result:

gcc version 4.2.4 (Ubuntu 4.2.4-1ubuntu4)

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detects the installed version of GNU GCC.

The script logs in via ssh, searches for executable 'gcc' and queries the found executables via command line option '-v'

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2015 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

GCC Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 806083

Vulnerability Detection Result:

Detected GNU GCC

Version: 4.2.4

Location: /usr/bin/gcc-4.2

CPE: cpe:/a:gnu:gcc:4.2.4

Concluded from version/product identification result:

gcc version 4.2.4 (Ubuntu 4.2.4-1ubuntu4)

Summary:

Detects the installed version of GNU GCC.

The script logs in via ssh, searches for executable 'gcc' and queries the found executables via command line option '-v'

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2015 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

GZip Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 800450

Vulnerability Detection Result:

Detected GZip

Version: 1.3.12

Location: /bin/gzip

CPE: cpe:/a:gnu:gzip:1.3.12

Concluded from version/product identification result:

gzip 1.3.12

Copyright (C) 2007 Free Software Foundation, Inc.

Copyright (C) 1993 Jean-loup Gailly.

This is free software. You may redistribute copies of it under the terms of the GNU General Public License <<http://www.gnu.org/licenses/gpl.html>>.

There is NO WARRANTY, to the extent permitted by law.

Written by Jean-loup Gailly.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Checks whether GZip is present on the target system and if so, tries to figure out the installed version.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (c) 2010 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

GZip Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 800450

Vulnerability Detection Result:

Detected GZip

Version: 1.2.4

Location: /usr/lib/klibc/bin/gzip

CPE: cpe:/a:gnu:gzip:1.2.4

Concluded from version/product identification result:

gzip 1.2.4 (18 Aug 93)

usage: gzip [-cdfhLnNtvV19] [-S suffix] [file ...]

-c --stdout write on standard output, keep original files unchanged  
-d --decompress decompress  
-f --force force overwrite of output file and compress links  
-h --help give this help  
-L --license display software license  
-n --no-name do not save or restore the original name and time stamp  
-N --name save or restore the original name and time stamp  
-q --quiet suppress all warnings  
-S .suf --suffix .suf use suffix .suf on compressed files  
-t --test test compressed file integrity  
-v --verbose verbose mode  
-V --version display version number  
file... files to decompress. If none given, use standard input.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Checks whether GZip is present on  
the target system and if so, tries to figure out the installed version.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (c) 2010 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

HTTP Security Headers Detection

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 112081

Vulnerability Detection Result:

Missing Headers | [More Information](#)

-----  
Content-Security-Policy | <https://owasp.org/www-project-secure-headers/#content-security-policy>

Feature-Policy | <https://owasp.org/www-project-secure-headers/#feature-policy>

Referrer-Policy | <https://owasp.org/www-project-secure-headers/#referrer-policy>

X-Content-Type-Options | <https://owasp.org/www-project-secure-headers/#x-content-type-options>

X-Frame-Options | <https://owasp.org/www-project-secure-headers/#x-frame-options>

X-Permitted-Cross-Domain-Policies |

<https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies>

X-XSS-Protection | <https://owasp.org/www-project-secure-headers/#x-xss-protection>

Summary:

All known security headers are being checked on the host. On completion a report

will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

<https://owasp.org/www-project-secure-headers/>

<https://owasp.org/www-project-secure-headers/#div-headers>

<https://securityheaders.io/>

CVSS Base Score: 0.0

Family name: General

Category: infos

Copyright: This script is Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-18T09:31:42+0000

Info:

HTTP Server Banner Enumeration

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 108708

Vulnerability Detection Result:

It was possible to enumerate the following HTTP server banner(s):

Server banner	Enumeration technique
---------------	-----------------------

Server: Apache/2.2.8 (Ubuntu) DAV/2   Valid HTTP 0.9 GET request to '/index.html'
---

X-Powered-By: PHP/5.2.4-2ubuntu5.10   Valid HTTP 0.9 GET request to '/index.php'
--

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2020 Greenbone Networks GmbH

Version: 2020-02-25T12:12:27+0000

Info:

HTTP Server type and version

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 10107

Vulnerability Detection Result:

The remote HTTP Server banner is:

Server: Apache/2.2.8 (Ubuntu) DAV/2

Summary:

This script detects and reports the HTTP Server's banner which might provide the type and version of it.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: Copyright (C) 2005 H. Scholz & Contributors

Version: 2020-02-06T14:44:42+0000

Info:

IRC Server Banner Detection

Risk: Info

Application: irc

Port: 6667

Protocol: tcp

ScriptID: 11156

Vulnerability Detection Result:

The IRC server banner is:

:irc.Metasploitable.LAN 351 BCCEGCDIC Unreal3.2.8.1. irc.Metasploitable.LAN :FhiXOoE [\*=2309]

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script tries to detect the banner of an IRC server.

CVSS Base Score: 0.0

Family name: Service detection

Category: unknown

Copyright: This script is Copyright (C) 2002 Michel Arboi

Version: \$Revision: 13541 \$

Info:

Apache Web Server Version Detection

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 900498

Vulnerability Detection Result:

Detected Apache HTTP/Web Server

Version: 2.2.8

Location: 80/tcp

CPE: cpe:/a:apache:http\_server:2.2.8

Concluded from version/product identification result:

Server: Apache/2.2.8

Summary:

Checks whether Apache HTTP/Web Server is present  
on the target system.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2020-03-04T13:56:06+0000

## Info:

### ISC BIND 'named' Detection (Remote)

Risk: Info

Application: domain

Port: 53

Protocol: tcp

ScriptID: 10028

Vulnerability Detection Result:

Detected ISC BIND

Version: 9.4.2

Location: 53/tcp

CPE: cpe:/a:isc:bind:9.4.2

Concluded from version/product identification result:

9.4.2

Insight:

The BIND based name servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send the information back to the querying source.

Solution:

Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

BIND 'named' is an open-source DNS server from isc.org. Many proprietary DNS servers are based on BIND source code.

References:

<https://www.isc.org/bind/>

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: This script is Copyright (C) 2005 SecuriTeam

Version: 2019-12-10T15:03:15+0000



Info:

jQuery Detection

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 141622

Vulnerability Detection Result:

Detected jQuery

Version: unknown

Location: /mutillidae/javascript/ddsmoothmenu

CPE: cpe:/a:jquery:jquery

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detection of jQuery.

The script sends a connection request to the server and attempts to detect jQuery and to extract its version.

References:

<https://jquery.com/>

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2018 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T07:32:24+0000

Info:

Kerberos5 Version Detection

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 800432

Vulnerability Detection Result:

Kerberos5 version 1.6.3 running at location /usr/bin/krb5-config was detected on the host

Summary:

This script detects the installed version of Kerberos5.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (c) 2010 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

SSH Authenticated Scan Info Consolidation

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 108162

Vulnerability Detection Result:

Description (Knowledge base entry) : Value/Content

Also use 'find' command to search for Applications enabled within 'Options for Local Security Checks'

(ssh/lsc/enable\_find) : yes

Amount of timeouts the 'find' command has reached. (ssh/lsc/find\_timeout) : None

Clear received buffer before sending a command (ssh/force/clear\_buffer) : FALSE

Commands are send via an pseudoterminal/pty (ssh/force/pty) : FALSE

Debugging enabled within 'Global variable settings' (global\_settings/ssh/debug) : FALSE

Descend directories on other filesystem enabled within 'Options for Local Security Checks' (ssh/lsc/descend\_ofs)

: yes

Don't prepend '/bin/sh -c' to used commands (ssh/force/nosh) : FALSE

Don't prepend 'LANG=C; LC\_ALL=C;' to the '/bin/sh -c' commands (ssh/force/nolang\_sh) :

FALSE

FreeBSD patchlevel (ssh/login/freebsdpatchlevel) : Not applicable for

target

FreeBSD release (ssh/login/freebsdrel) : Not applicable for

target

Login on a system with a restricted shell (ssh/restricted\_shell) : FALSE

Login on a system without common commands like 'cat' or 'find' (ssh/no\_linux\_shell) :

FALSE

Login via SSH failed (login/SSH/failed) : FALSE

Login via SSH successful (login/SSH/success) : TRUE

Mac OS X build (ssh/login/osx\_build) : Not applicable for

target

Mac OS X release name (ssh/login/osx\_name) : Not applicable for

target

Mac OS X version (ssh/login/osx\_version) : Not applicable for

target

Misconfigured CISCO device. No autocommand should be configured for the scanning user.

(ssh/cisco/broken\_autocommand) : FALSE

OpenBSD version (ssh/login/openbsdversion) : Not applicable for

target

Operating System Key used (ssh/login/release) : UBUNTU8.04 LTS

Port used for authenciated scans (kb\_ssh\_transport()) : 22/tcp

Report vulnerabilities of inactive Linux Kernel(s) separately. (ssh/login/kernel\_reporting\_overwrite/enabled) :

FALSE

Response to 'uname -a' command (ssh/login/uname) : Linux

metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

Send an extra command (ssh/send\_extra\_cmd) : FALSE

Solaris hardware type (ssh/login/solhardwaretype) : Not applicable for

target

Solaris version (ssh/login/solosversion) : Not applicable for target

User used for authenciated scans (kb\_ssh\_login()) : msfadmin

locate: Command available (ssh/locate/available)

: TRUE

rpm: Access to the RPM database failed (ssh/login/failed\_rpm\_db\_access)

: FALSE

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script consolidates various technical information about  
authenticated scans via SSH for Linux/UNIX targets.

References:

[https://docs.greenbone.net/GSM-Manual/gos-4/en/vulnerabilitymanagement.html#requirements-on-target-systems-wi](https://docs.greenbone.net/GSM-Manual/gos-4/en/vulnerabilitymanagement.html#requirements-on-target-systems-with-linux-unix)  
th-linux-unix

<https://docs.greenbone.net/GSM-Manual/gos-5/en/scanning.html#requirements-on-target-systems-with-linux-unix>

<https://docs.greenbone.net/GSM-Manual/gos-6/en/scanning.html#requirements-on-target-systems-with-linux-unix>

CVSS Base Score: 0.0

Family name: General

Category: end

Copyright: Copyright (C) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-20T12:10:27+0000

Info:

Microsoft SMB Signing Disabled

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 802726

Vulnerability Detection Result:

SMB signing is disabled on this host

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Checking for SMB signing is disabled.

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

CVSS Base Score: 0.0

Family name: Windows

Category: infos

Copyright: Copyright (c) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 11003 \$

Info:

Microsoft Windows SMB Accessible Shares

Risk: Info

Application: microsoft-ds

Port: 445

Protocol: tcp

ScriptID: 902425

Vulnerability Detection Result:

The following shares were found

IPC\$

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

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

CVSS Base Score: 0.0

Family name: Windows

Category: infos

Copyright: Copyright (c) 2012 SecPod

Summary: NOSUMMARY

Version: \$Revision: 11420 \$

Info:

Mozilla Firefox Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 800017

Vulnerability Detection Result:

Detected Firefox

Version: 3.6.17

Location: /usr/lib/firefox-3.6.17/firefox

CPE: cpe:/a:mozilla:firefox:3.6.17

Concluded from version/product identification result:

3.6.17

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script finds the Mozilla Firefox  
installed version on Linux.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2008 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

Sun Java Products Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 800385

Vulnerability Detection Result:

Detected Java LibGCJ version: 1.5.0

Location: /usr/bin/java

Concluded from version identification result:

java full version "gcj-1.5.0"

Summary:

Detects the installed version of Java products

on Linux systems. It covers the following:

- Sun Java
- Oracle Java
- IBM Java
- GCJ

The script logs in via ssh, searches for executables 'javaaws' and

'java' and queries the found executables via command line option '-fullversion'.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

Sun Java Products Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 800385

Vulnerability Detection Result:

Detected Java LibGCJ version: 1.5.0

Location: /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/bin/java

Concluded from version identification result:

java full version "gcj-1.5.0"

Summary:

Detects the installed version of Java products

on Linux systems. It covers the following:

- Sun Java
- Oracle Java
- IBM Java
- GCJ

The script logs in via ssh, searches for executables 'javaaws' and

'java' and queries the found executables via command line option '-fullversion'.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

Apache JServ Protocol v1.3 Detection

Risk: Info

Application: ajp13

Port: 8009

Protocol: tcp

ScriptID: 108082

Vulnerability Detection Result:

A service supporting the Apache JServ Protocol (AJP) v1.3 seems to be running on this port.

Summary:

The script detects a service supporting the

Apache JServ Protocol (AJP) version 1.3.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: Copyright (c) 2017 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-02T11:38:26+0000

Info:

Sun Java Products Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 800385

Vulnerability Detection Result:

Detected Java LibGCJ version: 1.5.0

Location: /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java

Concluded from version identification result:

java full version "gcj-1.5.0"

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detects the installed version of Java products

on Linux systems. It covers the following:

- Sun Java
- Oracle Java
- IBM Java
- GCJ

The script logs in via ssh, searches for executables 'javaaws' and

'java' and queries the found executables via command line option '-fullversion'.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000



Info:

MySQL/MariaDB Detection

Risk: Info

Application: mysql

Port: 3306

Protocol: tcp

ScriptID: 100152

Vulnerability Detection Result:

Detected MySQL

Version: 5.0.51a-3ubuntu5

Location: 3306/tcp

CPE: cpe:/a:mysql:mysql:5.0.51a

Concluded from version/product identification result:

5.0.51a-3ubuntu5

Summary:

Detects the installed version of

MySQL/MariaDB.

Detect a running MySQL/MariaDB by getting the banner, extract the version from the banner.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-11-05T16:13:01+0000

## Info:

Obtain list of all port mapper registered programs via RPC

Risk: Info

Application: rpcbind

Port: 111

Protocol: tcp

ScriptID: 11111

Vulnerability Detection Result:

These are the registered RPC programs:

RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/TCP

RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/TCP

RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/TCP

RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/TCP

RPC program #100021 version 1 'nlockmgr' on port 39163/TCP

RPC program #100021 version 3 'nlockmgr' on port 39163/TCP

RPC program #100021 version 4 'nlockmgr' on port 39163/TCP

RPC program #100024 version 1 'status' on port 41955/TCP

RPC program #100005 version 1 'mountd' (mount showmount) on port 52827/TCP

RPC program #100005 version 2 'mountd' (mount showmount) on port 52827/TCP

RPC program #100005 version 3 'mountd' (mount showmount) on port 52827/TCP

RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/UDP

RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/UDP

RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/UDP

RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/UDP

RPC program #100005 version 1 'mountd' (mount showmount) on port 38896/UDP

RPC program #100005 version 2 'mountd' (mount showmount) on port 38896/UDP

RPC program #100005 version 3 'mountd' (mount showmount) on port 38896/UDP

RPC program #100024 version 1 'status' on port 45773/UDP

RPC program #100021 version 1 'nlockmgr' on port 60018/UDP

RPC program #100021 version 3 'nlockmgr' on port 60018/UDP

RPC program #100021 version 4 'nlockmgr' on port 60018/UDP

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

CVSS Base Score: 0.0

Family name: RPC

Category: unknown

Copyright: This script is Copyright (C) 2002 Michel Arboi

Version: \$Revision: 13541 \$

## Info:

### OpenSSH Detection Consolidation

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 108577

Vulnerability Detection Result:

Detected OpenSSH Client

Version: 4.7p1

Location: /usr/bin/ssh

CPE: cpe:/a:openbsd:openssh:4.7p1

Concluded from version/product identification result:

OpenSSH\_4.7p1 Debian-8ubuntu1, OpenSSL 0.9.8g 19 Oct 2007

Detected OpenSSH Server

Version: 4.7p1

Location: /usr/sbin/sshd

CPE: cpe:/a:openbsd:openssh:4.7p1

Concluded from version/product identification result:

OpenSSH\_4.7p1 Debian-8ubuntu1, OpenSSL 0.9.8g 19 Oct 2007

Detected OpenSSH Server

Version: 4.7p1

Location: 22/tcp

CPE: cpe:/a:openbsd:openssh:4.7p1

Concluded from version/product identification result:

SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu1

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

The script reports a detected OpenSSH including the version number.

References:

<https://www.openssh.com/>

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: 2019-05-23T06:42:35+0000

Info:

OpenSSL Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 800335

Vulnerability Detection Result:

Detected OpenSSL

Version: 0.9.8g

Location: /usr/bin/openssl

CPE: cpe:/a:openssl:openssl:0.9.8g

Concluded from version/product identification result:

OpenSSL 0.9.8g

Summary:

Detects the installed version of OpenSSL.

The script logs in via ssh, searches for executable 'openssl' and queries the found executables via command line option 'version'.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

OS Detection Consolidation and Reporting

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 105937

Vulnerability Detection Result:

Best matching OS:

OS: Ubuntu

Version: 8.04

CPE: cpe:/o:canonical:ubuntu\_linux:8.04::-lts

Found by NVT: 1.3.6.1.4.1.25623.1.0.50282 (Determine OS and list of installed packages via SSH login)

Concluded from SSH login

Setting key "Host/runs\_unixoide" based on this information

Other OS detections (in order of reliability):

OS: Ubuntu

Version: 8.04

CPE: cpe:/o:canonical:ubuntu\_linux:8.04

Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)

Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu1

OS: Linux/Unix

CPE: cpe:/o:linux:kernel

Found by NVT: 1.3.6.1.4.1.25623.1.0.105355 (FTP OS Identification)

Concluded from FTP banner on port 21/tcp: 220 (vsFTPd 2.3.4)

OS: Debian GNU/Linux

CPE: cpe:/o:debian:debian\_linux

Found by NVT: 1.3.6.1.4.1.25623.1.0.105355 (FTP OS Identification)

Concluded from FTP banner on port 2121/tcp: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.56.12]

OS: Debian GNU/Linux

CPE: cpe:/o:debian:debian\_linux

Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)

Concluded from SMB/Samba banner on port 445/tcp:

OS String: Unix

SMB String: Samba 3.0.20-Debian

OS: Ubuntu

CPE: cpe:/o:canonical:ubuntu\_linux

Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)

Concluded from PHP Server banner on port 80/tcp: X-Powered-By: PHP/5.2.4-2ubuntu5.10

OS: Ubuntu

CPE: cpe:/o:canonical:ubuntu\_linux

Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)

Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.2.8 (Ubuntu) DAV/2

OS: Ubuntu

CPE: cpe:/o:canonical:ubuntu\_linux

Found by NVT: 1.3.6.1.4.1.25623.1.0.111068 (SMTP/POP3/IMAP Server OS Identification)

Concluded from SMTP banner on port 25/tcp: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

OS: Ubuntu

Version: 8.04

CPE: cpe:/o:canonical:ubuntu\_linux:8.04

Found by NVT: 1.3.6.1.4.1.25623.1.0.111069 (Telnet OS Identification)

Concluded from Telnet banner on port 23/tcp:

— — — — —

Version: 2020-03-30T08:21:10+0000

Info:

Perl Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 108503

Vulnerability Detection Result:

Detected Perl

Version: 5.8.8

Location: /usr/bin/perl

CPE: cpe:/a:perl:perl:5.8.8

Concluded from version/product identification result:

This is perl, v5.8.8

Summary:

Detects via SSH if Perl is installed on the target host.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2018 Greenbone Networks GmbH

Version: 2020-03-27T14:05:33+0000

Info:

Perl Modules Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 108504

Vulnerability Detection Result:

Detected Perl Module CGI

Version: 3.15

Location: /usr/bin/perl

CPE: cpe:/a:andy\_armstrong:cgi.pm:3.15

Concluded from version/product identification result:

3.15

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detects the version of various installed Perl modules via SSH.

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2018 Greenbone Networks GmbH

Version: \$Revision: 12740 \$

Info:

Perl Modules Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 108504

Vulnerability Detection Result:

Detected Perl Module Safe

Version: 2.29

Location: /usr/bin/perl

CPE: cpe:/a:rafael\_garcia-suarez:safe:2.29

Concluded from version/product identification result:  
2.29

Summary:

Detects the version of various installed Perl  
modules via SSH.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2018 Greenbone Networks GmbH

Version: \$Revision: 12740 \$

Info:

PHP Version Detection (Linux, local)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 103592

Vulnerability Detection Result:

Detected PHP

Version: 5.2.4-2ubuntu5.10

Location: /usr/bin/php

CPE: cpe:/a:php:php:5.2.4

Concluded from version/product identification result:  
PHP 5.2.4-2ubuntu5.10

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script finds the installed PHP version on Linux.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000



Info:

PHP Version Detection (Linux, local)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 103592

Vulnerability Detection Result:

Detected PHP

Version: 5.2.4-2ubuntu5.10

Location: /usr/bin/php5

CPE: cpe:/a:php:php:5.2.4

Concluded from version/product identification result:

PHP 5.2.4-2ubuntu5.10

Summary:

This script finds the installed PHP version on Linux.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

PHP Version Detection (Remote)

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 800109

Vulnerability Detection Result:

Detected PHP

Version: 5.2.4

Location: 80/tcp

CPE: cpe:/a:php:php:5.2.4

Concluded from version/product identification result:

X-Powered-By: PHP/5.2.4-2ubuntu5.10

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detects the installed version of PHP.

This script sends an HTTP GET request and tries to get the version from the response.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2008 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2019-12-17T14:07:10+0000

Info:

phpMyAdmin Detection

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 900129

Vulnerability Detection Result:

Detected phpMyAdmin

Version: 3.1.1

Location: /phpMyAdmin

CPE: cpe:/a:phpmyadmin:phpmyadmin:3.1.1

Concluded from version/product identification result:

Version 3.1.1

Concluded from version/product identification location:

http://192.168.56.12/phpMyAdmin/README

Extra information:

- Protected by Username/Password

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detection of phpMyAdmin.

The script sends a connection request to the server and attempts to extract the version number from the reply.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2008 SecPod

Summary: NOSUMMARY

Version: 2019-12-04T13:23:25+0000

Info:

Pidgin Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 900661

Vulnerability Detection Result:

Detected Pidgin version: 2.5.2

Location: /usr/bin/pidgin

CPE: cpe:/a:pidgin:pidgin:2.5.2

Concluded from version identification result:

Pidgin 2.5.2

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Detects the installed version of Pidgin.

The script logs in via ssh, searches for executable 'pidgin' and queries the found executables via command line option '--version'.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

Ping Host

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 100315

Vulnerability Detection Result:

The alive test was not launched because no method was selected.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This check tries to determine whether a remote host is up (alive).

Several methods are used for this depending on configuration of this check. Whether a host is up can be detected in 3 different ways:

- A ICMP message is sent to the host and a response is taken as alive sign.
- An ARP request is sent and a response is taken as alive sign.
- A number of typical TCP services (namely the 20 top ports of nmap) are tried and their presence is taken as alive sign.

None of the methods is failsafe. It depends on network and/or host configurations whether they succeed or not. Both, false positives and false negatives can occur.

Therefore the methods are configurable.

If you select to not mark unreachable hosts as dead, no alive detections are executed and the host is assumed to be available for scanning.

In case it is configured that hosts are never marked as dead, this can cause considerable timeouts and therefore a long scan duration in case the hosts are in fact not available.

The available methods might fail for the following reasons:

- ICMP: This might be disabled for a environment and would then cause false negatives as hosts are believed to be dead that actually are alive. In contrast it is also possible that a Firewall between the scanner and the target host is answering to the ICMP message and thus hosts are believed to be alive that actually are dead.
- TCP ping: Similar to the ICMP case a Firewall between the scanner and the target might answer to the sent probes and thus hosts are believed to be alive that actually are dead.

CVSS Base Score: 0.0

Family name: Port scanners

Category: scanner

Copyright: This script is Copyright (C) 2009, 2014, 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-03-26T16:09:27+0000

Info:

Postfix SMTP Server Detection

Risk: Info

Application: smtp

Port: 25

Protocol: tcp

ScriptID: 111086

Vulnerability Detection Result:

Detected Postfix

Version: unknown

Location: 25/tcp

CPE: cpe:/a:postfix:postfix

Concluded from version/product identification result:

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

The script checks the SMTP server  
banner for the presence of Postfix.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: This script is Copyright (C) 2016 SCHUTZWERK GmbH

Summary: NOSUMMARY

Version: 2020-03-23T13:51:29+0000

Info:

PostgreSQL Detection

Risk: Info

Application: postgres

Port: 5432

Protocol: tcp

ScriptID: 100151

Vulnerability Detection Result:

Detected PostgreSQL

Version: 8.3.1

Location: 5432/tcp

CPE: cpe:/a:postgresql:postgresql:8.3.1

Concluded from version/product identification result:

8.3.1

Summary:

Detection of PostgreSQL, a open source object-relational database system.

The script sends a connection request to the server (user:postgres, DB:postgres) and attempts to extract the version number from the reply.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

References:

<https://www.postgresql.org/>

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: This script is Copyright (C) 2009, 2011 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: 2020-02-26T09:22:27+0000

Info:

PostgreSQL Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 900478

Vulnerability Detection Result:

Detected PostgreSQL

Version: 8.3.1

Location: /usr/bin/psql

CPE: cpe:/a:postgresql:postgresql:8.3.1

Concluded from version/product identification result:

psql (PostgreSQL) 8.3.1

contains support for command-line editing

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Checks whether PostgreSQL is present on  
the target system and if so, tries to figure out the installed version.

References:

<https://www.postgresql.org/>

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

## Info:

### CGI Scanning Consolidation

Risk: Info

Application: http

Port: 80

Protocol: tcp

ScriptID: 111038

### Vulnerability Detection Result:

The Hostname/IP "192.168.56.12" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.

Requests to this service are done via HTTP/1.1.

This service seems to be able to host PHP scripts.

This service seems to be NOT able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

The following directories were used for CGI scanning:

http://192.168.56.12/

http://192.168.56.12/cgi-bin

http://192.168.56.12/dav

http://192.168.56.12/doc

http://192.168.56.12/dvwa

http://192.168.56.12/mutillidae

http://192.168.56.12/mutillidae/documentation

http://192.168.56.12/oops/TWiki

http://192.168.56.12/phpMyAdmin

http://192.168.56.12/rdiff/TWiki

http://192.168.56.12/test

http://192.168.56.12/test/testoutput

http://192.168.56.12/tikiwiki

http://192.168.56.12/tikiwiki/lib

http://192.168.56.12/twiki

http://192.168.56.12/twiki/pub

http://192.168.56.12/twiki/pub/TWiki/FileAttachment

http://192.168.56.12/twiki/pub/TWiki/TWikiDocGraphics

http://192.168.56.12/twiki/pub/TWiki/TWikiLogos

http://192.168.56.12/twiki/pub/TWiki/TWikiPreferences

http://192.168.56.12/twiki/pub/TWiki/TWikiTemplates

http://192.168.56.12/twiki/pub/icn

http://192.168.56.12/view/TWiki

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: `"/(index\.php|image|img|css|js$|js|/javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media|/skins?/)"`

http://192.168.56.12/icons

http://192.168.56.12/mutillidae/images

http://192.168.56.12/mutillidae/javascript

http://192.168.56.12/mutillidae/javascript/ddsmoothmenu



http://192.168.56.12/mutillidae/styles  
http://192.168.56.12/mutillidae/styles/ddsmoothmenu  
http://192.168.56.12/phpMyAdmin/themes/original/img  
http://192.168.56.12/tikiwiki/img/icons  
http://192.168.56.12/tikiwiki/styles  
http://192.168.56.12/tikiwiki/styles/transitions

Directory index found at:

http://192.168.56.12/dav/  
http://192.168.56.12/mutillidae/documentation/  
http://192.168.56.12/test/  
http://192.168.56.12/test/testoutput/  
http://192.168.56.12/twiki/TWikiDocumentation.html  
http://192.168.56.12/twiki/bin/view/TWiki/TWikiDocumentation  
http://192.168.56.12/twiki/bin/view/TWiki/TWikiInstallationGuide

Extraneous phpinfo() script found at:

http://192.168.56.12/mutillidae/phpinfo.php  
http://192.168.56.12/phpinfo.php

PHP script discloses physical path at:

http://192.168.56.12/tikiwiki/tiki-install.php (/var/www/tikiwiki/lib/adodb/drivers/adodb-mysql.inc.php)

The "Number of pages to mirror" setting (Current: 200) of the NVT "Web mirroring" (OID: 1.3.6.1.4.1.25623.1.0.10662) was reached. Raising this limit allows to mirror this host more thoroughly but might increase the scanning time.

NOTE: The 'Maximum number of items shown for each list' setting has been reached. There are 368 additional entries available for the following truncated list.

The following CGIs were discovered:

Syntax : cginame (arguments [default value])

http://192.168.56.12/dav/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )  
http://192.168.56.12/mutillidae/ (page [add-to-your-blog.php] )  
http://192.168.56.12/mutillidae/documentation/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )  
http://192.168.56.12/mutillidae/index.php (username [anonymous] do [toggle-hints] page [home.php] )  
http://192.168.56.12/oops/TWiki/TWikiHistory (template [oopsrev] param1 [1.10] )  
http://192.168.56.12/phpMyAdmin/index.php (phpMyAdmin [ad004ef3dbfde40b7989ba64a098b181eb682174] token [a5d5ef785d021970ed394866839e31ed] pma\_username [] table [] lang [] server [1] db [] convcharset [utf-8] pma\_password [] )  
http://192.168.56.12/phpMyAdmin/phpmyadmin.css.php (token [a5d5ef785d021970ed394866839e31ed] js\_frame [right] lang [en-utf-8] nocache [2457687151] convcharset [utf-8] )  
http://192.168.56.12/rdiff/TWiki/TWikiHistory (rev1 [1.10] rev2 [1.9] )  
http://192.168.56.12/test/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )  
http://192.168.56.12/test/testoutput/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )  
http://192.168.56.12/tikiwiki/tiki-install.php (host [localhost] dbinfo [] pass [] name [] db [] restart [1] resetdb [] user [] )  
http://192.168.56.12/twiki/bin/attach/TWiki/FileAttachment (filename [Sample.txt] revInfo [1] )  
http://192.168.56.12/twiki/bin/edit/Know/ReadmeFirst (t [1587100298] )  
http://192.168.56.12/twiki/bin/edit/Know/WebChanges (t [1587100148] )  
http://192.168.56.12/twiki/bin/edit/Know/WebHome (t [1587100109] )  
http://192.168.56.12/twiki/bin/edit/Know/WebIndex (t [1587100299] )  
http://192.168.56.12/twiki/bin/edit/Know/WebNotify (t [1587100301] )  
http://192.168.56.12/twiki/bin/edit/Know/WebPreferences (t [1587100155] )  
http://192.168.56.12/twiki/bin/edit/Know/WebSearch (t [1587100153] )  
http://192.168.56.12/twiki/bin/edit/Know/WebStatistics (t [1587100302] )  
http://192.168.56.12/twiki/bin/edit/Know/WebTopicList (t [1587100300] )  
http://192.168.56.12/twiki/bin/edit/Main/BillClinton (topicparent [Main.TWikiUsers] )  
http://192.168.56.12/twiki/bin/edit/Main/CharleytheHorse (t [1587100313] )  
http://192.168.56.12/twiki/bin/edit/Main/ChristopheVermeulen (topicparent [Main.TWikiUsers] )

<http://192.168.56.12/twiki/bin/edit/Main/DavidWarman> (topicparent [Main.TWikiUsers] )  
<http://192.168.56.12/twiki/bin/edit/Main/EngineeringGroup> (topicparent [Main.TWikiGroups] )  
<http://192.168.56.12/twiki/bin/edit/Main/GoodStyle> (topicparent [Main.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Main/JohnAltstadt> (topicparent [Main.TWikiUsers] )  
<http://192.168.56.12/twiki/bin/edit/Main/JohnTalintyre> (t [1587100314] )  
<http://192.168.56.12/twiki/bin/edit/Main/LondonOffice> (t [1587100323] )  
<http://192.168.56.12/twiki/bin/edit/Main/MartinRaabe> (topicparent [TWiki.TWikiUpgradeGuide] )  
<http://192.168.56.12/twiki/bin/edit/Main/NicholasLee> (t [1587100315] )  
<http://192.168.56.12/twiki/bin/edit/Main/OfficeLocations> (t [1587100117] )  
<http://192.168.56.12/twiki/bin/edit/Main/PeterFokkinga> (topicparent [Main.TWikiUsers] )  
<http://192.168.56.12/twiki/bin/edit/Main/PeterThoeny> (t [1587100215] )  
<http://192.168.56.12/twiki/bin/edit/Main/SanJoseOffice> (t [1587100322] )  
<http://192.168.56.12/twiki/bin/edit/Main/SupportGroup> (topicparent [Main.TWikiGroups] )  
<http://192.168.56.12/twiki/bin/edit/Main/TWikiAdminGroup> (t [1587100319] )  
<http://192.168.56.12/twiki/bin/edit/Main/TWikiGroups> (t [1587100116] )  
<http://192.168.56.12/twiki/bin/edit/Main/TWikiGuest> (t [1587100315] )  
<http://192.168.56.12/twiki/bin/edit/Main/TWikiPreferences> (topicparent [Main.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Main/TWikiRegistration> (topicparent [Main.TWikiUsers] )  
<http://192.168.56.12/twiki/bin/edit/Main/TWikiUsers> (t [1587100114] )  
<http://192.168.56.12/twiki/bin/edit/Main/TWikiWeb> (topicparent [Main.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Main/TestArea> (topicparent [Main.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Main/TextFormattingFAQ> (topicparent [Main.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Main/TextFormattingRules> (topicparent [Main.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Main/TokyoOffice> (t [1587100323] )  
<http://192.168.56.12/twiki/bin/edit/Main/WebChanges> (t [1587100119] )  
<http://192.168.56.12/twiki/bin/edit/Main/WebHome> (t [1587100096] )  
<http://192.168.56.12/twiki/bin/edit/Main/WebIndex> (t [1587100124] )  
<http://192.168.56.12/twiki/bin/edit/Main/WebNotify> (t [1587100161] )  
<http://192.168.56.12/twiki/bin/edit/Main/WebPreferences> (t [1587100129] )  
<http://192.168.56.12/twiki/bin/edit/Main/WebSearch> (t [1587100126] )  
<http://192.168.56.12/twiki/bin/edit/Main/WebStatistics> (t [1587100162] )  
<http://192.168.56.12/twiki/bin/edit/Main/WebTopicEditTemplate> (topicparent [Main.WebPreferences] )  
<http://192.168.56.12/twiki/bin/edit/Main/WebTopicList> (t [1587100161] )  
<http://192.168.56.12/twiki/bin/edit/Main/WelcomeGuest> (topicparent [Main.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Main/WikiName> (topicparent [Main.TWikiUsers] )  
<http://192.168.56.12/twiki/bin/edit/Main/WikiNotation> (topicparent [Main.TWikiUsers] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/TestTopic1> (topicparent [Sandbox.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/TestTopic2> (topicparent [Sandbox.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/TestTopic3> (topicparent [Sandbox.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/TestTopic4> (topicparent [Sandbox.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/TestTopic5> (topicparent [Sandbox.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/TestTopic6> (topicparent [Sandbox.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/TestTopic7> (topicparent [Sandbox.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/TestTopic8> (topicparent [Sandbox.WebHome] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/WebChanges> (t [1587100156] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/WebHome> (t [1587100110] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/WebIndex> (t [1587100304] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/WebNotify> (t [1587100310] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/WebPreferences> (t [1587100159] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/WebSearch> (t [1587100158] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/WebStatistics> (t [1587100311] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/WebTopicEditTemplate> (topicparent [Sandbox.WebPreferences] )  
<http://192.168.56.12/twiki/bin/edit/Sandbox/WebTopicList> (t [1587100309] )

[http://192.168.56.12/twiki/bin/edit/TWiki/ \(topic \[\] topicparent \[TWikiFAQ\] onlywikiname \[on\] templatetopic \[TWikiFaqTemplate\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/ (topic [] topicparent [TWikiFAQ] onlywikiname [on] templatetopic [TWikiFaqTemplate] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/AppendixFileSystem \(t \[1587100287\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/AppendixFileSystem (t [1587100287] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/BumpyWord \(t \[1587100325\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/BumpyWord (t [1587100325] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/DefaultPlugin \(t \[1587100240\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/DefaultPlugin (t [1587100240] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/FileAttachment \(t \[1587100234\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/FileAttachment (t [1587100234] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/FormattedSearch \(t \[1587100267\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/FormattedSearch (t [1587100267] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/GnuGeneralPublicLicense \(t \[1587100294\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/GnuGeneralPublicLicense (t [1587100294] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/GoodStyle \(t \[1587100204\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/GoodStyle (t [1587100204] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/InstalledPlugins \(t \[1587100291\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/InstalledPlugins (t [1587100291] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/InstantEnhancements \(t \[1587100245\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/InstantEnhancements (t [1587100245] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/InterWikis \(t \[1587100242\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/InterWikis (t [1587100242] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/InterwikiPlugin \(t \[1587100241\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/InterwikiPlugin (t [1587100241] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/ManagingTopics \(t \[1587100283\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/ManagingTopics (t [1587100283] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/ManagingWebs \(t \[1587100285\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/ManagingWebs (t [1587100285] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/MeaningfulTitle \(topicparent \[TWiki.TextFormattingFAQ\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/MeaningfulTitle (topicparent [TWiki.TextFormattingFAQ] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/NewTopic \(topicparent \[TWiki.TWikiShorthand\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/NewTopic (topicparent [TWiki.TWikiShorthand] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/NotExistingYet \(topicparent \[TWiki.TextFormattingRules\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/NotExistingYet (topicparent [TWiki.TextFormattingRules] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/PeterThoeny \(t \[1587100293\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/PeterThoeny (t [1587100293] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/SiteMap \(t \[1587100292\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/SiteMap (t [1587100292] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/StartingPoints \(t \[1587100132\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/StartingPoints (t [1587100132] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/TWikiAccessControl \(t \[1587100259\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/TWikiAccessControl (t [1587100259] ))

[http://192.168.56.12/twiki/bin/edit/TWiki/TWikiAdminCookBook \(t \[1587100243\] \)](http://192.168.56.12/twiki/bin/edit/TWiki/TWikiAdminCookBook (t [1587100243] ))

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

The script consolidates various information for CGI scanning.

This information is based on the following scripts / settings:

- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI\_Directory\_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi\_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use

If you think any of this information is wrong please report it to the referenced community portal.

References:

<https://community.greenbone.net/c/vulnerability-tests>

CVSS Base Score: 0.0

Family name: Web application abuses

Category: infos

Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH

Summary: NOSUMMARY

Version: 2019-09-23T09:25:24+0000

Info:

PostgreSQL Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 900478

Vulnerability Detection Result:

Detected PostgreSQL

Version: 8.3.1

Location: /usr/lib/postgresql/8.3/bin/psql

CPE: cpe:/a:postgresql:postgresql:8.3.1

Concluded from version/product identification result:

psql (PostgreSQL) 8.3.1

contains support for command-line editing

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Checks whether PostgreSQL is present on  
the target system and if so, tries to figure out the installed version.

References:

<https://www.postgresql.org/>

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

ProFTPD Server Version Detection (Local)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 900506

Vulnerability Detection Result:

Detected ProFTPD

Version: 1.3.1

Location: /usr/sbin/proftpd

CPE: cpe:/a:proftpd:proftpd:1.3.1

Concluded from version/product identification result:

1.3.1

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script detects the installed version of ProFTPD Server.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2020-03-27T14:05:33+0000

Info:

ProFTPD Server Version Detection (Remote)

Risk: Info

Application: unknown

Port: 2121

Protocol: tcp

ScriptID: 900815

Vulnerability Detection Result:

Detected ProFTPD

Version: 1.3.1

Location: 2121/tcp

CPE: cpe:/a:proftpd:proftpd:1.3.1

Concluded from version/product identification result:

220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.56.12]

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script detects the installed version of ProFTP Server.

CVSS Base Score: 0.0

Family name: Product detection

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2020-03-24T12:27:11+0000

Info:

Python Version Detection (Linux)

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 113560

Vulnerability Detection Result:

Detected Python

Version: 2.5.2

Location: /usr/bin/python

CPE: cpe:/a:python:python:2.5.2

Concluded from version/product identification result:

Python 2.5.2

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

Checks whether Python is present on  
the target system and if so, tries to figure out the installed version.

References:

<https://www.python.org/>

CVSS Base Score: 0.0

Family name: Product detection

Category: unknown

Copyright: Copyright (C) 2019 Greenbone Networks GmbH

Version: 2020-03-27T14:05:33+0000

Info:

Report running Kernel

Risk: Info

Application: general

Port: 0

Protocol: tcp

ScriptID: 105885

Vulnerability Detection Result:

The remote host is running Linux Kernel "2.6.24-16-server".

Concluded from uname: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:

This script reports the running kernel.

CVSS Base Score: 0.0

Family name: General

Category: infos

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 11885 \$

Info:

RMI-Registry Detection

Risk: Info

Application: unknown

Port: 1099

Protocol: tcp

ScriptID: 105839

Vulnerability Detection Result:

The RMI-Registry Service is running at this port

Summary:

This Script detects the RMI-Registry Service

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: Service detection

Category: infos

Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH

Summary: NOSUMMARY

Version: \$Revision: 13541 \$

Info:

RPC portmapper (TCP)

Risk: Info

Application: rpcbind

Port: 111

Protocol: tcp

ScriptID: 108090

Vulnerability Detection Result:

RPC portmapper is running on this port.

Summary:

This script performs detection of RPC portmapper on TCP.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0

Family name: RPC

Category: infos

Copyright: Copyright (C) 2009 SecPod

Summary: NOSUMMARY

Version: 2020-03-26T06:41:35+0000