Nessus Report

Report

21/Mar/2012:09:07:06 GMT
<table>
<thead>
<tr>
<th>Vulnerability Id</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>55407 (1)</td>
<td>USN-1149-1 : firefox, xulrunner-1.9.2 vulnerabilities</td>
</tr>
<tr>
<td>56860 (1)</td>
<td>USN-1263-1 : icedtea-web, openjdk-6, openjdk-6b18 vulnerabilities</td>
</tr>
<tr>
<td>57685 (1)</td>
<td>USN-1263-2 : openjdk-6, openjdk-6b18 regression</td>
</tr>
<tr>
<td>55976 (1)</td>
<td>Apache HTTP Server Byte Range DoS</td>
</tr>
<tr>
<td>58325 (1)</td>
<td>USN-1397-1 : mysql-5.1, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities</td>
</tr>
<tr>
<td>57792 (3)</td>
<td>Apache HTTP Server httpOnly Cookie Information Disclosure</td>
</tr>
<tr>
<td>18262 (1)</td>
<td>TFTP Traversal Arbitrary File Access</td>
</tr>
<tr>
<td>18405 (1)</td>
<td>Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness</td>
</tr>
<tr>
<td>43156 (1)</td>
<td>NTP ntpd Mode 7 Error Response Packet Loop Remote DoS</td>
</tr>
<tr>
<td>45374 (1)</td>
<td>AFP Server Directory Traversal</td>
</tr>
<tr>
<td>55114 (1)</td>
<td>USN-1148-1 : libmodplug vulnerabilities</td>
</tr>
<tr>
<td>42880 (1)</td>
<td>SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection</td>
</tr>
<tr>
<td>53491 (1)</td>
<td>SSL / TLS Renegotiation DoS</td>
</tr>
<tr>
<td>10394 (2)</td>
<td>Microsoft Windows SMB Log In Possible</td>
</tr>
<tr>
<td>10859 (1)</td>
<td>Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration</td>
</tr>
<tr>
<td>10860 (1)</td>
<td>SMB Use Host SID to Enumerate Local Users</td>
</tr>
</tbody>
</table>
Vulnerabilities By Plugin
Synopsis
The remote Ubuntu host is missing one or more security-related patches.

Description
Multiple memory vulnerabilities were discovered in the browser rendering engine. An attacker could use these to possibly execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2364, CVE-2011-2365, CVE-2011-2374, CVE-2011-2376)
Martin Barbella discovered that under certain conditions, viewing a XUL document while JavaScript was disabled caused deleted memory to be accessed. An attacker could potentially use this to crash Firefox or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2373) Jordi Chancel discovered a vulnerability on multipart/x-mixed-replace images due to memory corruption. An attacker could potentially use this to crash Firefox or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2377) Chris Rohlf and Yan Ivnitskiy discovered an integer overflow vulnerability in JavaScript Arrays. An attacker could potentially use this to execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2371)
Multiple use-after-free vulnerabilities were discovered. An attacker could potentially use these to execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-0083, CVE-2011-0085, CVE-2011-2363)
David Chan discovered that cookies did not honor same-origin conventions. This could potentially lead to cookie data being leaked to a third party. (CVE-2011-2362)

See Also
http://www.ubuntu.com/usn/usn-1149-1/

Solution
Update the affected package(s).

Risk Factor
Critical

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

References
CVE CVE-2011-0083
CVE CVE-2011-0085
CVE CVE-2011-2362
CVE CVE-2011-2363
CVE CVE-2011-2364
CVE CVE-2011-2365
CVE CVE-2011-2371
CVE CVE-2011-2373
CVE CVE-2011-2374
CVE CVE-2011-2376
CVE CVE-2011-2377
XREF USN:1149-1

Exploitable with
Metasploit (true)

Hosts
192.168.1.248 (tcp/0)
- Installed package: xulrunner-1.9.2_1.9.2.17+build3+nobinonly-ubuntu0.10.04.1
Fixed package: xulrunner-1.9.2_1.9.2.18+build2+nobinonly-ubuntu0.10.04.1
Synopsis

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

Description

Deepak Bhole discovered a flaw in the Same Origin Policy (SOP) implementation in the IcedTea web browser plugin. This could allow a remote attacker to open connections to certain hosts that should not be permitted. (CVE-2011-3377)

Juliano Rizzo and Thai Duong discovered that the block-wise AES encryption algorithm block-wise as used in TLS/SSL was vulnerable to a chosen-plaintext attack. This could allow a remote attacker to view confidential data. (CVE-2011-3389)

It was discovered that a type confusion flaw existed in the Internet Inter-Orb Protocol (IIOP) deserialization code. A remote attacker could use this to cause an untrusted application or applet to execute arbitrary code by deserializing malicious input. (CVE-2011-3521)

It was discovered that the Java scripting engine did not perform SecurityManager checks. This could allow a remote attacker to cause an untrusted application or applet to execute arbitrary code with the full privileges of the JVM. (CVE-2011-3544)

It was discovered that the InputStream class used a global buffer to store input bytes skipped. An attacker could possibly use this to gain access to sensitive information. (CVE-2011-3547)

It was discovered that a vulnerability existed in the AWTKeyStroke class. A remote attacker could cause an untrusted application or applet to execute arbitrary code. (CVE-2011-3548)

It was discovered that an integer overflow vulnerability existed in the TransformHelper class in the Java2D implementation. A remote attacker could use this to cause a denial of service via an application or applet crash or possibly execute arbitrary code. (CVE-2011-3551)

It was discovered that the default number of available UDP sockets for applications running under SecurityManager restrictions was set too high. A remote attacker could use this with a malicious application or applet exhaust the number of available UDP sockets to cause a denial of service for other applets or applications running within the same JVM. (CVE-2011-3552)

It was discovered that Java API for XML Web Services (JAX-WS) could incorrectly expose a stack trace. A remote attacker could potentially use this to gain access to sensitive information. (CVE-2011-3553)

It was discovered that the unpacker for pack200 JAR files did not sufficiently check for errors. An attacker could cause a denial of service or possibly execute arbitrary code through a specially crafted pack200 JAR file. (CVE-2011-3554)

It was discovered that the RMI registration implementation did not properly restrict privileges of remotely executed code. A remote attacker could use this to execute code with elevated privileges. (CVE-2011-3556, CVE-2011-3557)

It was discovered that the HotSpot VM could be made to crash, allowing an attacker to cause a denial of service or possibly leak sensitive information. (CVE-2011-3558)

It was discovered that the HttpsURLConnection class did not properly perform SecurityManager checks in certain situations. This could allow a remote attacker to bypass restrictions on HTTPS connections. (CVE-2011-3560)

See Also

http://www.ubuntu.com/usn/usn-1263-1/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

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

References

CVE
CVE-2011-3377
CVE-2011-3389
CVE-2011-3521
CVE-2011-3544
| CVE     | CVE-2011-3547 |
| CVE     | CVE-2011-3548 |
| CVE     | CVE-2011-3551 |
| CVE     | CVE-2011-3552 |
| CVE     | CVE-2011-3553 |
| CVE     | CVE-2011-3554 |
| CVE     | CVE-2011-3556 |
| CVE     | CVE-2011-3557 |
| CVE     | CVE-2011-3558 |
| CVE     | CVE-2011-3560 |

**XREF**

| IAVA:2011-A-0142 |
| IAVA:2012-A-0004 |
| IAVA:2011-A-0155 |

**Exploitable with**

CANVAS (true) Metasploit (true)

**Hosts**

192.168.1.248 (tcp/0)

- Installed package: icedtea-6-jre-cacao_6b20-1.9.7-0ubuntu1-10.04.1
  Fixed package: icedtea-6-jre-cacao_6b20-1.9.10-0ubuntu1-10.04.2

- Installed package: openjdk-6-jre_6b20-1.9.7-0ubuntu1-10.04.1
  Fixed package: openjdk-6-jre_6b20-1.9.10-0ubuntu1-10.04.2

- Installed package: openjdk-6-jre-headless_6b20-1.9.7-0ubuntu1-10.04.1
  Fixed package: openjdk-6-jre-headless_6b20-1.9.10-0ubuntu1-10.04.2

- Installed package: openjdk-6-jre-lib_6b20-1.9.7-0ubuntu1-10.04.1
  Fixed package: openjdk-6-jre-lib_6b20-1.9.10-0ubuntu1-10.04.2
The remote Ubuntu host is missing one or more security-related patches.

USN-1263-1 fixed vulnerabilities in OpenJDK 6. The upstream patch for the chosen plaintext attack on the block-wise AES encryption algorithm (CVE-2011-3389) introduced a regression that caused TLS/SSL connections to fail when using certain algorithms. This update fixes the problem.

We apologize for the inconvenience.

Original advisory details:
Deepak Bhole discovered a flaw in the Same Origin Policy (SOP) implementation in the IcedTea web browser plugin. This could allow a remote attacker to open connections to certain hosts that should not be permitted. (CVE-2011-3377) Juliano Rizzo and Thai Duong discovered that the block-wise AES encryption algorithm block-wise as used in TLS/SSL was vulnerable to a chosen-plaintext attack. This could allow a remote attacker to view confidential data. (CVE-2011-3389) It was discovered that a type confusion flaw existed in the Internet Inter-Orb Protocol (IIOP) deserialization code. A remote attacker could use this to cause an untrusted application or applet to execute arbitrary code by deserializing malicious input. (CVE-2011-3521) It was discovered that the Java scripting engine did not perform SecurityManager checks. This could allow a remote attacker to cause an untrusted application or applet to execute arbitrary code with the full privileges of the JVM. (CVE-2011-3544) It was discovered that the InputStream class used a global buffer to store input bytes skipped. An attacker could possibly use this to gain access to sensitive information. (CVE-2011-3547) It was discovered that a vulnerability existed in the AWTKeyStroke class. A remote attacker could cause an untrusted application or applet to execute arbitrary code. (CVE-2011-3548) It was discovered that an integer overflow vulnerability existed in the TransformHelper class in the Java2D implementation. A remote attacker could use this cause a denial of service via an application or applet crash or possibly execute arbitrary code. (CVE-2011-3551) It was discovered that the default number of available UDP sockets for applications running under SecurityManager restrictions was set too high. A remote attacker could use this with a malicious application or applet exhaust the number of available UDP sockets to cause a denial of service for other applets or applications running within the same JVM. (CVE-2011-3552) It was discovered that Java API for XML Web Services (JAX-WS) could incorrectly expose a stack trace. A remote attacker could potentially use this to gain access to sensitive information. (CVE-2011-3553) It was discovered that the unpacker for pack200 JAR files did not sufficiently check for errors. An attacker could cause a denial of service or possibly execute arbitrary code through a specially crafted pack200 JAR file. (CVE-2011-3554) It was discovered that the RMI registration implementation did not properly restrict privileges of remotely executed code. A remote attacker could use this to execute code with elevated privileges. (CVE-2011-3556, CVE-2011-3557) It was discovered that the HotSpot VM could be made to crash, allowing an attacker to cause a denial of service or possibly leak sensitive information. (CVE-2011-3558) It was discovered that the HttpsURLConnection class did not properly perform SecurityManager checks in certain situations. This could allow a remote attacker to bypass restrictions on HTTPS connections. (CVE-2011-3560)

CVE-2011-3548
CVE-2011-3551
CVE-2011-3552
CVE-2011-3553
CVE-2011-3554
CVE-2011-3556
CVE-2011-3557
CVE-2011-3558
CVE-2011-3559
CVE-2011-3560

**Exploitable with**
- CANVAS (true)
- Metasploit (true)

**Hosts**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Port</th>
<th>Installed Package</th>
<th>Fixed Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.248</td>
<td>tcp/0</td>
<td>icedtea-6-jre-cacao_6b20-1.9.7-0ubuntu1-10.04.1</td>
<td>icedtea-6-jre-cacao_6b20-1.9.10-0ubuntu1-10.04.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>openjdk-6-jre_6b20-1.9.7-0ubuntu1-10.04.1</td>
<td>openjdk-6-jre_6b20-1.9.10-0ubuntu1-10.04.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>openjdk-6-jre-headless_6b20-1.9.7-0ubuntu1-10.04.1</td>
<td>openjdk-6-jre-headless_6b20-1.9.10-0ubuntu1-10.04.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>openjdk-6-jre-lib_6b20-1.9.7-0ubuntu1-10.04.1</td>
<td>openjdk-6-jre-lib_6b20-1.9.10-0ubuntu1-10.04.3</td>
</tr>
</tbody>
</table>
Synopsis
The web server running on the remote host is affected by a denial of service vulnerability.

Description
The version of Apache HTTP Server running on the remote host is affected by a denial of service vulnerability. Making a series of HTTP requests with overlapping ranges in the Range or Request-Range request headers can result in memory and CPU exhaustion. A remote, unauthenticated attacker could exploit this to make the system unresponsive. Exploit code is publicly available and attacks have reportedly been observed in the wild.

See Also
http://www.gossamer-threads.com/lists/apache/dev/401638
http://httpd.apache.org/security/CVE-2011-3192.txt
http://www.01.ibm.com/support/docview.wss?uid=swg24030863

Solution
Upgrade to Apache httpd 2.2.21 or later, or use one of the workarounds in Apache's advisories for CVE-2011-3192. Version 2.2.20 fixed the issue, but also introduced a regression.
If the host is running a web server based on Apache httpd, contact the vendor for a fix.

Risk Factor
High

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

CVSS Temporal Score
6.4 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

References
BID 49303
CVE CVE-2011-3192
XREF OSVDB:74721
XREF CERT:405811
XREF EDB-ID:17696
XREF EDB-ID:18221
XREF IAVA:2011-A-0120
XREF IAVA:2011-A-0130
XREF IAVA:2011-A-0141

Hosts
192.168.1.248 (tcp/80)
Nessus determined the server is unpatched and is not using any of the suggested workarounds by making the following requests:

------------------------ Testing for workarounds ------------------------
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:

See Also
http://www.ubuntu.com/usn/usn-1397-1/

Solution
Update the affected package(s).

Risk Factor
High

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

References
CVE CVE-2007-5925
CVE CVE-2008-3963
CVE CVE-2008-4098
CVE CVE-2008-4456
CVE CVE-2008-7247
CVE CVE-2009-2446
CVE CVE-2009-4019
CVE CVE-2009-4030
CVE CVE-2009-4484
CVE CVE-2010-1621
CVE CVE-2010-1626
CVE CVE-2010-1848
CVE CVE-2010-1849
CVE CVE-2010-1850
CVE CVE-2010-2008
CVE CVE-2010-3677
CVE CVE-2010-3678
CVE-2010-3679
CVE-2010-3680
CVE-2010-3681
CVE-2010-3682
CVE-2010-3683
CVE-2010-3833
CVE-2010-3834
CVE-2010-3835
CVE-2010-3836
CVE-2010-3837
CVE-2010-3838
CVE-2010-3839
CVE-2010-3840
CVE-2011-2262
CVE-2012-0075
CVE-2012-0087
CVE-2012-0101
CVE-2012-0102
CVE-2012-0112
CVE-2012-0113
CVE-2012-0114
CVE-2012-0115
CVE-2012-0116
XREF
USN:1397-1
XREF
CWE:119

Exploitable with
CANVAS (true)Core Impact (true)Metasploit (true)

Hosts
192.168.1.248 (tcp/0)

- Installed package : mysql-server-5.1_5.1.41-3ubuntu12.10
  Fixed package     : mysql-server-5.1_5.1.61-0ubuntu0.10.04.1
57792 (3) - Apache HTTP Server httpOnly Cookie Information Disclosure

Synopsis
The web server running on the remote host has an information disclosure vulnerability.

Description
The version of Apache HTTP Server running on the remote host has an information disclosure vulnerability. Sending a request with HTTP headers long enough to exceed the server limit causes the web server to respond with an HTTP 400. By default, the offending HTTP header and value are displayed on the 400 error page. When used in conjunction with other attacks (e.g., cross-site scripting), this could result in the compromise of httpOnly cookies.

See Also
http://fd.the-wildcat.de/apache_e36a9cf46c.php
http://httpd.apache.org/security/vulnerabilities_22.html
http://svn.apache.org/viewvc?view=revision&revision=1235454

Solution
Upgrade to Apache version 2.2.22 or later.

Risk Factor
Medium

CVSS Base Score
4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score
3.6 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References
BID 51706
CVE CVE-2012-0053
XREF OSVDB:78556
XREF EDB-ID:18442
XREF IAVA:2012-A-0017

Hosts
192.168.1.30 (tcp/80)
192.168.1.30 (tcp/443)
192.168.1.248 (tcp/80)
The remote TFTP server can be used to read arbitrary files on the remote host.

The TFTP (Trivial File Transfer Protocol) server running on the remote host is vulnerable to a directory traversal attack that allows an attacker to read arbitrary files on the remote host by prepending their names with directory traversal sequences.

Disable the remote TFTP daemon, run it in a chrooted environment, or filter incoming traffic to this port.

Medium

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

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

6198

11582

11584

33287

33344

42907

48272

50441

CVE-1999-0183

CVE-1999-0498

CVE-2002-2353

CVE-2009-0271

CVE-2009-0288

CVE-2009-1161

OSVDB:8069

OSVDB:11221

OSVDB:11297

OSVDB:11349

OSVDB:51404

OSVDB:51487
It was possible to retrieve the contents of the file /etc/passwd from the remote host:

```
root:x:0:0:root:/root:/bin/sh
dao:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:33:33:sys:/dev:/bin/sh
sync:x:4:100:sync:/bin:/bin/sync
mail:x:8:8:mail:/var/spool/mail:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
operator:x:37:37:Operator:/var:/bin/sh
sshd:x:103:99:Operator:/var:/bin/sh
nobody:x:99:99:nobody:/home:/bin/sh
default:x:1000:1000:Default non-root user:/home/default:/bin/sh
```
### Synopsis

It may be possible to get access to the remote host.

### Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hardcoded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

### See Also


### Solution

- Force the use of SSL as a transport layer for this service if supported, or/and
- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

### Risk Factor

Medium

### CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

### CVSS Temporal Score

4.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

### References

<table>
<thead>
<tr>
<th>BID</th>
<th>13818</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>CVE-2005-1794</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:17131</td>
</tr>
</tbody>
</table>

### Hosts

192.168.1.16 (tcp/3389)
### Synopsis
The remote network time service has a denial of service vulnerability.

### Description
The version of ntpd running on the remote host has a denial of service vulnerability. It responds to mode 7 error packets with its own mode 7 error packets. A remote attacker could exploit this by sending a mode 7 error response with a spoofed IP header, setting the source and destination IP addresses to the IP address of the target. This would cause ntpd to respond to itself endlessly, consuming excessive amounts of CPU, resulting in a denial of service.

### See Also
- https://support.ntp.org/bugs/show_bug.cgi?id=1331
- http://www.nessus.org/u?3a07ed05

### Solution
Upgrade to NTP 4.2.4p8 or later.

### Risk Factor
Medium

### CVSS Base Score
6.4 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:P)

### CVSS Temporal Score
5.3 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:P)

### References
- **BID**: 37255
- **CVE**: CVE-2009-3563
- **XREF**: OSVDB:60847
- **XREF**: CERT:568372
- **XREF**: Secunia:37629

### Hosts
**192.168.1.211 (udp/123)**
**45374 (1) - AFP Server Directory Traversal**

**Synopsis**
The remote service is vulnerable to an information disclosure attack.

**Description**
The remote AFP server allows guest users to read files located outside public shares by sending requests to the `..` directory.
An attacker could use this flaw to read every file on this host.

**See Also**
http://support.apple.com/kb/HT4077


http://www.securityfocus.com/advisories/19364

**Solution**
Upgrade to Mac OS X 10.6.3 or apply Security Update 2010-002.

**Risk Factor**
Medium

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

**CVSS Temporal Score**
4.1 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

**References**

<table>
<thead>
<tr>
<th>BID</th>
<th>CVE</th>
<th>XREF</th>
</tr>
</thead>
<tbody>
<tr>
<td>39020</td>
<td>CVE-2010-0533</td>
<td>OSVDB:63366</td>
</tr>
</tbody>
</table>

**Hosts**

**192.168.1.30 (tcp/548)**

It was possible to obtain a listing of `..' for the share 'media' :
- lost+found
- backup
- home
- .timemachine
- .vault
- media
- aquota.group
- aquota.user
The remote Ubuntu host is missing one or more security-related patches.

It was discovered that libmodplug did not correctly handle certain malformed S3M media files. If a user or automated system were tricked into opening a crafted S3M file, an attacker could cause a denial of service or possibly execute arbitrary code with privileges of the user invoking the program. (CVE-2011-1574)

It was discovered that libmodplug did not correctly handle certain malformed ABC media files. If a user or automated system were tricked into opening a crafted ABC file, an attacker could cause a denial of service or possibly execute arbitrary code with privileges of the user invoking the program. (CVE-2011-1761)

The default compiler options for affected releases should reduce the vulnerability to a denial of service.

See Also
http://www.ubuntu.com/usn/usn-1148-1/

Solution
Update the affected package(s).

Risk Factor
Medium

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

References
CVE CVE-2011-1574
CVE CVE-2011-1761
XREF USN:1148-1

Exploitable with
CANVAS (true) Metasploit (true)

Hosts
192.168.1.248 (tcp/0)

- Installed package : libmodplug0c2_1:0.8.7-1build1
  Fixed package     : libmodplug0c2_1:0.8.7-1ubuntu0.2
### Synopsis
The remote service allows insecure renegotiation of TLS / SSL connections.

### Description
The remote service encrypts traffic using TLS / SSL but allows a client to insecurely renegotiate the connection after the initial handshake. An unauthenticated, remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer.

### See Also
- [http://www.kb.cert.org/vuls/id/120541](http://www.kb.cert.org/vuls/id/120541)
- [http://www.g-sec.lu/practicaltls.pdf](http://www.g-sec.lu/practicaltls.pdf)

### Solution
Contact the vendor for specific patch information.

### Risk Factor
Low

### CVSS Base Score
2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

### CVSS Temporal Score
2.1 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

### References

<table>
<thead>
<tr>
<th>BID</th>
<th>36935</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>CVE-2009-3555</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:59968</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:59969</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:59970</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:59971</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:59972</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:59973</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:59974</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:60366</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:60521</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:61234</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:61718</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB:61784</td>
</tr>
<tr>
<td>XREF</td>
<td>OSVDB</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td>61785</td>
</tr>
<tr>
<td></td>
<td>61929</td>
</tr>
<tr>
<td></td>
<td>62064</td>
</tr>
<tr>
<td></td>
<td>62135</td>
</tr>
<tr>
<td></td>
<td>62210</td>
</tr>
<tr>
<td></td>
<td>62273</td>
</tr>
<tr>
<td></td>
<td>62536</td>
</tr>
<tr>
<td></td>
<td>62877</td>
</tr>
<tr>
<td></td>
<td>64040</td>
</tr>
<tr>
<td></td>
<td>64499</td>
</tr>
<tr>
<td></td>
<td>64725</td>
</tr>
<tr>
<td></td>
<td>65202</td>
</tr>
<tr>
<td></td>
<td>66315</td>
</tr>
<tr>
<td></td>
<td>67029</td>
</tr>
<tr>
<td></td>
<td>69032</td>
</tr>
<tr>
<td></td>
<td>69561</td>
</tr>
<tr>
<td></td>
<td>70055</td>
</tr>
<tr>
<td></td>
<td>70620</td>
</tr>
<tr>
<td></td>
<td>71951</td>
</tr>
<tr>
<td></td>
<td>71961</td>
</tr>
<tr>
<td></td>
<td>74335</td>
</tr>
<tr>
<td></td>
<td>75622</td>
</tr>
<tr>
<td></td>
<td>77832</td>
</tr>
<tr>
<td></td>
<td>IAVA:2009-A-0122</td>
</tr>
<tr>
<td></td>
<td>IAVA:2010-A-0047</td>
</tr>
<tr>
<td></td>
<td>IAVA:2010-A-0048</td>
</tr>
<tr>
<td></td>
<td>IAVA:2010-A-0072</td>
</tr>
<tr>
<td></td>
<td>IAVA:2010-A-0089</td>
</tr>
<tr>
<td></td>
<td>IAVA:2010-A-0108</td>
</tr>
<tr>
<td></td>
<td>IAVA:2010-A-0149</td>
</tr>
<tr>
<td></td>
<td>IAVA:2010-A-0155</td>
</tr>
</tbody>
</table>
Hosts
192.168.1.81 (tcp/443)

Port 443 supports insecure renegotiation over TLSv1.
### Synopsis
The remote service allows repeated renegotiation of TLS / SSL connections.

### Description
The remote service encrypts traffic using TLS / SSL and permits clients to renegotiate connections. The computational requirements for renegotiating a connection are asymmetrical between the client and the server, with the server performing several times more work. Since the remote host does not appear to limit the number of renegotiations for a single TLS / SSL connection, this permits a client to open several simultaneous connections and repeatedly renegotiate them, possibly leading to a denial of service condition.

### See Also
- [http://www.ietf.org/mail-archive/web/tls/current/msg07553.html](http://www.ietf.org/mail-archive/web/tls/current/msg07553.html)

### Solution
Contact the vendor for specific patch information.

### Risk Factor
Low

### CVSS Base Score
2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:N/A:P)

### CVSS Temporal Score
2.3 (CVSS2#AV:N/AC:H/Au:N/C:N/I:N/A:P)

### References
- **BID**: 48626
- **CVE**: CVE-2011-1473
- **XREF**: OSVDB:73894

### Hosts
**192.168.1.13 (tcp/1243)**

Port 1243 is vulnerable to renegotiation DoS over TLSv1.
**10394 (2) - Microsoft Windows SMB Log In Possible**

**Synopsis**
It is possible to log into the remote host.

**Description**
The remote host is running Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts:
- NULL session
- Guest account
- Given Credentials

**See Also**
http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

**Solution**
n/a

**Risk Factor**
None

**Exploitable with**
Metasploit (true)

**Hosts**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Service</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.16 (tcp/445)</td>
<td></td>
<td>- NULL sessions are enabled on the remote host</td>
</tr>
<tr>
<td>192.168.1.30 (tcp/445)</td>
<td></td>
<td>- NULL sessions are enabled on the remote host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Remote users are authenticated as 'Guest'</td>
</tr>
</tbody>
</table>
### Synopsis
It is possible to obtain the host SID for the remote host.

### Description
By emulating the call to `LsaQueryInformationPolicy()`, it was possible to obtain the host SID (Security Identifier). The host SID can then be used to get the list of local users.

### See Also

### Solution
You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.
Refer to the 'See also' section for guidance.

### Risk Factor
None

### Hosts
192.168.1.30 (tcp/445)

The remote host SID value is:
1-5-21-3581115777-3128578739-639081464

The value of 'RestrictAnonymous' setting is: unknown
### Synopsis
It is possible to enumerate local users.

### Description
Using the host security identifier (SID), it is possible to enumerate local users on the remote Windows system.

### Solution
n/a

### Risk Factor
None

### Hosts
**192.168.1.30 (tcp/445)**

- nobody (id 501, Guest account)
- admin (id 1196)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.