Marek Muusikus

CVE-2013-7100

Referaat aines „Andmeturve“

Juhendaja:

Meelis Roos

TARTU

2014
Table of Contents

Introduction ............................................................................................................................. 3
Description .............................................................................................................................. 3
Fix......................................................................................................................................... 4
References ............................................................................................................................. 5
**Introduction**

Asterisk is an open source project that powers IP PBX, VoIP gateways, call center systems, conference bridges, voicemail servers and all kinds of other applications that involve real-time communications. [1]

CVE-2013-7100 was reported on September 26, 2013 by Jan Juergens. A 16-bit SMS message with an odd number of bytes causes buffer overflow, which allows remote attackers to cause a denial of service. [2] [3]

**Description**

Affected versions (table taken from [2]):

<table>
<thead>
<tr>
<th>Product</th>
<th>Release series</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asterisk Open Source</td>
<td>1.8.x</td>
<td>All Versions</td>
</tr>
<tr>
<td>Asterisk Open Source</td>
<td>10.x</td>
<td>All Versions</td>
</tr>
<tr>
<td>Asterisk with Digiumphones</td>
<td>10.x-digiumphones</td>
<td>All Versions</td>
</tr>
<tr>
<td>Asterisk Open Source</td>
<td>11.x</td>
<td>All Versions</td>
</tr>
<tr>
<td>Certified Asterisk</td>
<td>1.8.x</td>
<td>All Versions</td>
</tr>
<tr>
<td>Certified Asterisk</td>
<td>11.x</td>
<td>All Versions</td>
</tr>
</tbody>
</table>

If a remote user sends a 16-bit SMS message that contains an odd message length value it will cause the message decoding loop to run forever (see the loop in the patch below). The message buffer will be overflowed resulting in corrupted memory and an immediate crash.
Fix

Here is a patch for Asterisk 1.8:

Index: apps/app_sms.c
===================================================================
--- apps/app_sms.c (revision 403852)
+++ apps/app_sms.c (revision 403853)
@@ -696,7 +696,7 @@
     while (l--)
         int v = *i++;
-    if (l--)
+    if (l && l--)
         v = (v << 8) + *i++;
     }    
     *o++ = v;
@@ -714,6 +714,7 @@
 } else if (is8bit(dcs)) {
     unpacksms8(i, l, udh, udhl, ud, udl, udhi);
 } else {
+    l += l % 2;
     unpacksms16(i, l, udh, udhl, ud, udl, udhi);
 }    
 return l + 1;

The function unpacksms16() always expects an even number of bytes to be processed. If, however, the user data header contains an odd number of bytes, the second while-loop never terminates (l is never 0 in the while condition). [4]

The idea of this patch is to check for an odd number of bytes and if so another byte will be added. It ensures that the message decoding loop will stop at the end of the received message.
References

1. http://www.asterisk.org/