### Product
Asterisk

### Summary
Remote crash vulnerability in IAX2 channel driver.

### Nature of Advisory
Remote crash

### Susceptibility
Established calls

### Severity
Moderate

### Exploits Known
No

### Reported On
March 21, 2012

### Reported By
mgrobecker

### Posted On
May 29, 2012

### Last Updated On
May 29, 2012

### Advisory Contact
Richard Mudgett < rmudgett AT digium DOT com >

### CVE Name
CVE-2012-2947

### Description
A remotely exploitable crash vulnerability exists in the IAX2 channel driver if an established call is placed on hold without a suggested music class. For this to occur, the following must take place:
1. The setting mohinterpret=passthrough must be set on the end placing the call on hold.
2. A call must be established.
3. The call is placed on hold without a suggested music-on-hold class name.

When these conditions are true, Asterisk will attempt to use an invalid pointer to a music-on-hold class name. Use of the invalid pointer will either cause a crash or the music-on-hold class name will be garbage.

### Resolution
Asterisk now sets the extra data parameter to null if the received control frame does not have any extra data.

### Affected Versions

<table>
<thead>
<tr>
<th>Product</th>
<th>Release Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certified Asterisk</td>
<td>1.8.11-cert</td>
</tr>
<tr>
<td>Asterisk Open Source</td>
<td>1.8.x</td>
</tr>
<tr>
<td>Asterisk Open Source</td>
<td>10.x</td>
</tr>
</tbody>
</table>
Asterisk Project Security Advisory - AST-2012-007

Corrected In

<table>
<thead>
<tr>
<th>Product</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certified Asterisk</td>
<td>1.8.11-cert2</td>
</tr>
<tr>
<td>Asterisk Open Source</td>
<td>1.8.12.1, 10.4.1</td>
</tr>
</tbody>
</table>

Patches

<table>
<thead>
<tr>
<th>SVN URL</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://downloads.asterisk.org/pub/security/AST-2012-007-1.8.11-cert.diff">http://downloads.asterisk.org/pub/security/AST-2012-007-1.8.11-cert.diff</a></td>
<td>v1.8.11-cert</td>
</tr>
<tr>
<td><a href="http://downloads.asterisk.org/pub/security/AST-2012-007-1.8.diff">http://downloads.asterisk.org/pub/security/AST-2012-007-1.8.diff</a></td>
<td>v1.8</td>
</tr>
<tr>
<td><a href="http://downloads.asterisk.org/pub/security/AST-2012-007-10.diff">http://downloads.asterisk.org/pub/security/AST-2012-007-10.diff</a></td>
<td>v10</td>
</tr>
</tbody>
</table>

Links

https://issues.asterisk.org/jira/browse/ASTERISK-19597

Asterisk Project Security Advisories are posted at http://www.asterisk.org/security
This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2012-007.pdf and http://downloads.digium.com/pub/security/AST-2012-007.html

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Editor</th>
<th>Revisions Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/29/2012</td>
<td>Richard Mudgett</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>