### Summary
Remote Crash Vulnerability in SIP channel driver

### Nature of Advisory
Remote attacker can crash an Asterisk server

### Susceptibility
Remote Authenticated Sessions

### Severity
Moderate

### Exploits Known
No

### Reported On
05/23/11

### Reported By
Jonathan Rose jrose@digium.com

### Posted On
06/02/11

### Last Updated On
06/02/11

### Advisory Contact
Jonathan Rose jrose@digium.com

### CVE Name
CVE-2011-2216

### Description
If a remote user initiates a SIP call and the recipient picks up, the remote user can reply with a malformed Contact header that Asterisk will improperly handle and cause a crash due to a segmentation fault.

### Resolution
Asterisk now immediately initializes buffer strings coming into the parse_uri_full function to prevent outside functions from receiving a NULL value pointer. This should increase the safety of any function that uses parse_uri or its wrapper functions which previously would attempt to work in the presence of a parse_uri failure by reading off of potentially uninitialized strings.
## Affected Versions

<table>
<thead>
<tr>
<th>Product</th>
<th>Release Series</th>
<th>Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asterisk Open Source</td>
<td>1.8.x</td>
<td>All versions</td>
</tr>
</tbody>
</table>

## Corrected In

<table>
<thead>
<tr>
<th>Product</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asterisk Open Source</td>
<td>1.8.4.2</td>
</tr>
</tbody>
</table>

## Patches

<table>
<thead>
<tr>
<th>URL</th>
<th>Branch</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="Http://downloads.asterisk.org/pub/security/AST-2011-007-1.8.diff">Http://downloads.asterisk.org/pub/security/AST-2011-007-1.8.diff</a></td>
<td>1.8</td>
</tr>
</tbody>
</table>


## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Editor</th>
<th>Revisions Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/02/11</td>
<td>Jonathan Rose</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>

Asterisk Project Security Advisory - AST-2011-007

Copyright © 2011 Digium, Inc. All Rights Reserved.

Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.