**Product** | Asterisk  
---|---  
**Summary** | Remote Crash Vulnerability in SIP channel driver  
**Nature of Advisory** | Remote attacker can crash an Asterisk server  
**Susceptibility** | Remote Unauthenticated Sessions  
**Severity** | Critical  
**Exploits Known** | Yes  
**Reported On** | 06/15/2011  
**Reported By** | Paul Belanger pabelanger@digium.com  
**Posted On** | 06/20/2011  
**Last Updated On** | June 16, 2011  
**Advisory Contact** | Kinsey Moore kmoore@digium.com  
**CVE Name** | CVE-2011-2529

**Description**  
If a remote user sends a SIP packet containing a null, Asterisk assumes available data extends past the null to the end of the packet when the buffer is actually truncated when copied. This causes SIP header parsing to modify data past the end of the buffer altering unrelated memory structures. This vulnerability does not affect TCP/TLS connections.

**Resolution**  
Asterisk now uses the correct length when dealing with SIP packets containing nulls. Available workarounds are to disable chan_sip or to upgrade.

| Affected Versions |
|---|---|
| **Product** | **Release Series** |
| Asterisk Open Source | 1.6.0.x All  
Asterisk Open Source | 1.6.1.x All  
Asterisk Open Source | 1.6.2.x All  
Asterisk Open Source | 1.8.x All |

| Corrected In |
|---|---|
| **Product** | **Release** |
| Asterisk Open Source 1.6.2.x | 1.6.2.18.1  
Asterisk Open Source 1.8.x | 1.8.4.3 |

Asterisk Project Security Advisory - AST-2011-008  
Copyright © 2011 Digium, Inc. All Rights Reserved.  
Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.
Asterisk Project Security Advisory - AST-2011-008

---

**Patches**

<table>
<thead>
<tr>
<th>URL</th>
<th>Branch</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="Http://downloads.asterisk.org/pub/security/AST-2011-008.diff">Http://downloads.asterisk.org/pub/security/AST-2011-008.diff</a></td>
<td>1.6.2, 1.8</td>
</tr>
</tbody>
</table>

Asterisk Project Security Advisories are posted at [http://www.asterisk.org/security](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This document may be superseded by later versions; if so, the latest version will be posted at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-2011-008.pdf](http://downloads.digium.com/pub/security/AST-2011-008.pdf) and [http://downloads.digium.com/pub/security/AST-2011-008.html](http://downloads.digium.com/pub/security/AST-2011-008.html)

---

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Editor</th>
<th>Revisions Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/20/2011</td>
<td>Kinsey Moore</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>

---

Copyright © 2011 Digium, Inc.  All Rights Reserved.
Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.