Asterisk Project Security Advisory - AST-2014-005

Product | Asterisk
---|---
Summary | Remote Crash in PJSIP Channel Driver's Publish/Subscribe Framework
Nature of Advisory | Denial of Service
Susceptibility | Remote Unauthenticated Sessions
Severity | Moderate
Exploits Known | No
Reported On | March 17, 2014
Reported By | John Bigelow <jbigelow AT digium DOT com>
Posted On | June 12, 2014
Last Updated On | June 12, 2014
Advisory Contact | Kevin Harwell <kharwell AT digium DOT com>
CVE Name | CVE-2014-4045

Description
A remotely exploitable crash vulnerability exists in the PJSIP channel driver's pub/sub framework. If an attempt is made to unsubscribe when not currently subscribed and the endpoint's “sub_min_expiry” is set to zero, Asterisk tries to create an expiration timer with zero seconds, which is not allowed, so an assertion raised.

Resolution
Upgrade to a version with the patch integrated, apply the patch, or make sure the “sub_min_expiry” endpoint configuration option is greater than zero.

Affected Versions

<table>
<thead>
<tr>
<th>Product</th>
<th>Release Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asterisk Open Source</td>
<td>12.x All</td>
</tr>
</tbody>
</table>

Corrected In

<table>
<thead>
<tr>
<th>Product</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asterisk Open Source 12.x</td>
<td>12.3.1</td>
</tr>
</tbody>
</table>

Patches

<table>
<thead>
<tr>
<th>SVN URL</th>
<th>Revision</th>
</tr>
</thead>
</table>

Asterisk Project Security Advisory - AST-2014-005
Copyright © 2014 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-2014-005

Links

https://issues.asterisk.org/jira/browse/ASTERISK-23489

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2014-005.pdf and http://downloads.digium.com/pub/security/AST-2014-005.html

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Editor</th>
<th>Revisions Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 14, 2014</td>
<td>Kevin Harwell</td>
<td>Document Creation</td>
</tr>
<tr>
<td>June 12, 2014</td>
<td>Matt Jordan</td>
<td>Added CVE</td>
</tr>
</tbody>
</table>

Copyright © 2014 Digium, Inc. All Rights Reserved.
Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.