<table>
<thead>
<tr>
<th><strong>Product</strong></th>
<th>Asterisk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>AMI permission escalation through DB dialplan function</td>
</tr>
<tr>
<td><strong>Nature of Advisory</strong></td>
<td>Permission Escalation</td>
</tr>
<tr>
<td><strong>Susceptibility</strong></td>
<td>Remote Authenticated Sessions</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Minor</td>
</tr>
<tr>
<td><strong>Exploits Known</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Reported On</strong></td>
<td>November 17, 2014</td>
</tr>
<tr>
<td><strong>Reported By</strong></td>
<td>Gareth Palmer</td>
</tr>
<tr>
<td><strong>Posted On</strong></td>
<td>20 November, 2014</td>
</tr>
<tr>
<td><strong>Last Updated On</strong></td>
<td>November 21, 2014</td>
</tr>
<tr>
<td><strong>Advisory Contact</strong></td>
<td>Kevin Harwell &lt;kharwell AT digium DOT com&gt;</td>
</tr>
<tr>
<td><strong>CVE Name</strong></td>
<td>CVE-2014-8418</td>
</tr>
</tbody>
</table>

**Description**
The DB dialplan function when executed from an external protocol (for instance AMI), could result in a privilege escalation.

**Resolution**
Asterisk now inhibits the DB function from being executed from an external interface if the live_dangerously option is set to no.

### Affected Versions

<table>
<thead>
<tr>
<th><strong>Product</strong></th>
<th><strong>Release Series</strong></th>
<th><strong>Affected Version</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Certified Asterisk</td>
<td>1.8</td>
<td>All versions</td>
</tr>
<tr>
<td>Certified Asterisk</td>
<td>11.6</td>
<td>All versions</td>
</tr>
<tr>
<td>Asterisk Open Source</td>
<td>1.8.x</td>
<td>All versions</td>
</tr>
<tr>
<td>Asterisk Open Source</td>
<td>11.x</td>
<td>All versions</td>
</tr>
<tr>
<td>Asterisk Open Source</td>
<td>12.x</td>
<td>All versions</td>
</tr>
<tr>
<td>Asterisk Open Source</td>
<td>13.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>1.8.32.1,11.14.1, 12.7.1, 13.0.1</td>
</tr>
<tr>
<td>Certified Asterisk</td>
<td>1.8.28-cert3,11.6-cert8</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-2014-018-1.8.28.diff">http://downloads.asterisk.org/pub/security/AST-2014-018-1.8.28.diff</a></td>
<td>Certified Asterisk 1.8</td>
</tr>
<tr>
<td><a href="http://downloads.asterisk.org/pub/security/AST-2014-018-1.8.diff">http://downloads.asterisk.org/pub/security/AST-2014-018-1.8.diff</a></td>
<td>Asterisk 1.8</td>
</tr>
</tbody>
</table>

### Links

| https://issues.asterisk.org/jira/browse/ASTERISK-24534                  |                                              |

Asterisk Project Security Advisories are posted at [http://www.asterisk.org/security](http://www.asterisk.org/security)

### Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Editor</th>
<th>Revisions Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 18, 2014</td>
<td>Kevin Harwell</td>
<td>Initial advisory created</td>
</tr>
</tbody>
</table>

Asterisk Project Security Advisory - AST-2014-018
Copyright © 2014 Digium, Inc. All Rights Reserved.
Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.