Asterisk Project Security Advisory – AST-2014-017

Product	Asterisk
Summary	Permission escalation through ConfBridge actions/dialplan functions
Nature of Advisory	Permission Escalation
Susceptibility	Remote Authenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	November 4, 2014
Reported By	Gareth Palmer
Posted On	20 November, 2014
Last Updated On	November 21, 2014
Advisory Contact	Kevin Harwell <kharwell AT digium DOT com>
CVE Name	CVE-2014-8417

Description	The CONFBRIDGE dialplan function when executed from an external protocol (for instance AMI), could result in a privilege escalation. Also, the AMI action “ConfbridgeStartRecord” could also be used to execute arbitrary system commands without first checking for system access.

Resolution	Asterisk now inhibits the CONFBRIDGE function from being executed from an external interface if the live_dangerously option is set to no. Also, the “ConfbridgeStartRecord” AMI action is now only allowed to execute under a user with system level access.

<table>
<tr><th colspan="3">Affected Versions</th></tr>
<tr><th>Product</th><th>Release Series</th><th></th></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>
<tr><td>Certified Asterisk</td><td>11.6</td><td>All versions</td></tr>
</table>

Corrected In	
Product	**Release**
Asterisk Open Source	11.14.1, 12.7.1, 13.0.1
Certified Asterisk	11.6-cert8

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2014-017-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2014-017-12.diff	Asterisk 12
http://downloads.asterisk.org/pub/security/AST-2014-017-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2014-017-11.6.diff	Certified Asterisk 11.6

Links	https://issues.asterisk.org/jira/browse/ASTERISK-24490

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2014-017.pdf and http://downloads.digium.com/pub/security/AST-2014-017.html

Revision History		
Date	**Editor**	**Revisions Made**
November 18, 2014	Kevin Harwell	Initial advisory created