Product	Asterisk
Summary	High call load may result in hung channels in ConfBridge.
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	19 October, 2014
Reported By	Ben Klang
Posted On	20 November 2014
Last Updated On	November 21, 2014
Advisory Contact	Joshua Colp <jcolp AT digium DOT com>
CVE Name	CVE-2014-8414

Description	The ConfBridge application uses an internal bridging API to implement conference bridges. This internal API uses a state model for channels within the conference bridge and transitions between states as different things occur. Under load it is possible for some state transitions to be delayed causing the channel to transition from being hung up to waiting for media. As the channel has been hung up remotely no further media will arrive and the channel will stay within ConfBridge indefinitely.

Resolution	The underlying bridging code that ConfBridge uses has been fixed so state changes can not occur that will take a channel out of the hung up state.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	11.x	All versions
Certified Asterisk	11.6	All versions

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

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/ AST-2014-014-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/ AST-2014-014-11.6.diff	Certified Asterisk 11.6

Links	https://issues.asterisk.org/jira/browse/ASTERISK-24440

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2014-014.pdf and http://downloads.digium.com/pub/security/AST-2014-014.html

Revision History		
Date	**Editor**	**Revisions Made**
20 November, 2014	Joshua Colp	Initial Advisory created