Product	Asterisk
Summary	Remote Crash Vulnerability in PJSIP channel driver
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	30 October 2014
Reported By	Yaron Nahum
Posted On	20 November 2014
Last Updated On	November 21, 2014
Advisory Contact	Joshua Colp <jcolp AT digium DOT com>
CVE Name	CVE-2014-8415

Description	The chan_pjsip channel driver uses a queue approach for actions relating to SIP sessions. There exists a race condition where actions may be queued to answer a session or send ringing AFTER a SIP session has been terminated using a CANCEL request. The code will incorrectly assume that the SIP session is still active and attempt to send the SIP response. The PJSIP library does not expect the SIP session to be in the disconnected state when sending the response and asserts.

Resolution	Asterisk has been patched so any queued actions that occur after a SIP session has been disconnected will not execute.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	12.x	All versions
Asterisk Open Source	13.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	12.7.1, 13.0.1

Patches

SVN URL	Revision
http://downloads.asterisk.org/pub/security/AST-2014-015-12.diff	Asterisk 12
http://downloads.asterisk.org/pub/security/AST-2014-015-13.diff	Asterisk 13

Links	https://issues.asterisk.org/jira/browse/ASTERISK-24471

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2014-015.pdf and http://downloads.digium.com/pub/security/AST-2014-015.html

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