Product	Asterisk
Summary	Remote Crash Vulnerability in PJSIP channel driver
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	17 November 2014
Reported By	Joshua Colp
Posted On	20 November 2014
Last Updated On	November 21, 2014
Advisory Contact	Joshua Colp <jcolp AT digium DOT com>
CVE Name	CVE-2014-8416

Description	When handling an INVITE with Replaces message the res_pjsip_refer module incorrectly assumes that it will be operating on a channel that has just been created. If the INVITE with Replaces message is sent in-dialog after a session has been established this assumption will be incorrect. The res_pjsip_refer module will then hang up a channel that is actually owned by another thread. When this other thread attempts to use the just hung up channel it will end up using freed channel which will likely cause a crash.

Resolution	If REFER support is not required the res_pjsip_refer module can be unloaded to limit exposure otherwise the res_pjsip_refer module has been patched so it will not allow an in-dialog INVITE with Replaces message to be processed.

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-2014-016-12.diff	Asterisk 12
http://downloads.asterisk.org/pub/security/AST-2014-016-13.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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2014-016.pdf and http://downloads.digium.com/pub/security/AST-2014-016.html

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