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	January 29, 2014
Reported By	Joshua Colp <jcolp AT digium DOT com>
Posted On	March 10, 2014
Last Updated On	March 10, 2014
Advisory Contact	Joshua Colp <jcolp AT digium DOT com>
CVE Name	CVE-2014-2288

Description	A remotely exploitable crash vulnerability exists in the PJSIP channel driver if the "qualify_frequency" configuration option is enabled on an AOR and the remote SIP server challenges for authentication of the resulting OPTIONS request. The response handling code wrongly assumes that a PJSIP endpoint will always be associated with an outgoing request which is incorrect.

Resolution	This patch adds a check when handling responses challenging for authentication. If no endpoint is associated with the request no retry with authentication will occur.

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

Corrected In	
Product	**Release**
Asterisk Open Source 12.x	12.1.1

Patches	
SVN URL	**Revision**

http://downloads.asterisk.org/pub/security/AST-2014-003-12.diff	Asterisk 12

Links	https://issues.asterisk.org/jira/browse/ASTERISK-23210

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2014-003.pdf and http://downloads.digium.com/pub/security/AST-2014-003.html

Revision History		
Date	**Editor**	**Revisions Made**
03/05/14	Joshua Colp	Document Creation