Product	Asterisk
Summary	Crash in PJSIP resource when missing a contact header
Nature of Advisory	Remote Crash
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	December 12, 2017
Reported By	Ross Beer
Posted On	
Last Updated On	December 22, 2017
Advisory Contact	Kevin Harwell <kharwell AT digium DOT com>
CVE Name	CVE-2017-17850

Description	A select set of SIP messages create a dialog in Asterisk. Those SIP messages must contain a contact header. For those messages, if the header was not present and using the PJSIP channel driver, it would cause Asterisk to crash. The severity of this vulnerability is somewhat mitigated if authentication is enabled. If authentication is enabled a user would have to first be authorized before reaching the crash point.

Resolution	When using the Asterisk PJSIP resource, and one of the SIP messages that create a dialog is received Asterisk now checks to see if the message contains a contact header. If it does not Asterisk now responds with a “400 Missing Contact header”.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	13.x	All versions
Asterisk Open Source	14.x	All versions
Asterisk Open Source	15.x	All versions
Certified Asterisk	13.18	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	13.18.5, 14.7.5, 15.1.5
Certified Asterisk	13.18-cert2

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2017-014-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2017-014-14.diff	Asterisk 14
http://downloads.asterisk.org/pub/security/AST-2017-014-15.diff	Asterisk 15
http://downloads.asterisk.org/pub/security/AST-2017-014-13.18.diff	Certified Asterisk 13.18

Links	https://issues.asterisk.org/jira/browse/ASTERISK-27480

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2017-014.pdf and http://downloads.digium.com/pub/security/AST-2017-014.html

Revision History		
Date	**Editor**	**Revisions Made**
December 20, 2017	Kevin Harwell	Initial Revision
December 22, 2017	Kevin Harwell	Updated with CVE