Asterisk Project Security Advisory - AST-2016-008

Product	Asterisk
Summary	Crash on SDP offer or answer from endpoint using Opus
Nature of Advisory	Remote Crash
Susceptibility	Remote unauthenticated sessions
Severity	Critical
Exploits Known	No
Reported On	November 11, 2016
Reported By	jorgen
Posted On	December 08, 2016
Last Updated On	December 13, 2016
Advisory Contact	jcolp AT digium DOT com
CVE Name	CVE-2016-9937

Description	If an SDP offer or answer is received with the Opus codec and with the format parameters separated using a space the code responsible for parsing will recursively call itself until it crashes. This occurs as the code does not properly handle spaces separating the parameters. This does NOT require the endpoint to have Opus configured in Asterisk. This also does not require the endpoint to be authenticated. If guest is enabled for chan_sip or anonymous in chan_pjsip an SDP offer or answer is still processed and the crash occurs.

Resolution	The code has been updated to properly handle spaces separating parameters in the fmtp line. Upgrade to a released version with the fix incorporated or apply patch.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	13.x	13.12.0 and higher
Asterisk Open Source	14.x	All Versions

Corrected In	
Product	**Release**
Asterisk Open Source	13.13.1, 14.2.1

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2016-008-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2016-008-14.diff	Asterisk 14

Links	https://issues.asterisk.org/jira/browse/ASTERISK-26579

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2016-008.pdf and http://downloads.digium.com/pub/security/AST-2016-008.html

Revision History		
Date	**Editor**	**Revisions Made**
November 15, 2016	Joshua Colp	Initial draft of Advisory
December 13, 2016	Kevin Harwell	Added CVE number