Product	Asterisk
Summary	Remote Crash Vulnerability in RTCP Stack
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	October 30, 2017
Reported By	Tzafrir Cohen and Vitezslav Novy
Posted On	December 13, 2017
Last Updated On	December 12, 2017
Advisory Contact	Jcolp AT digium DOT com
CVE Name	

Description	If a compound RTCP packet is received containing more than one report (for example a Receiver Report and a Sender Report) the RTCP stack will incorrectly store report information outside of allocated memory potentially causing a crash. For all versions of Asterisk this vulnerability requires an active call to be established. For versions of Asterisk 13.17.2, 14.6.2, 15.0.0, 13.13-cert6 and greater an additional level of security is placed upon RTCP packets. If the probation period for incoming RTP traffic has passed any received RTCP packets must contain the same SSRC as the RTP traffic. If the RTCP packets do not then they are dropped. This ensures other parties can not inject RTCP packets without they themselves establishing an active call.

Resolution	The RTCP stack has been changed so the report information is always stored in allocated memory. The provided patches can be applied to the appropriate version or the latest version of Asterisk can be installed to receive the fix.

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	13.13	All Versions

Corrected In	
Product	**Release**
Asterisk Open Source	13.18.4, 14.7.4, 15.1.4
Certified Asterisk	13.13-cert9

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2017-012-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2017-012-14.diff	Asterisk 14
http://downloads.asterisk.org/pub/security/AST-2017-012-15.diff	Asterisk 15
http://downloads.asterisk.org/pub/security/AST-2017-012-13.13.diff	Certified Asterisk 13.13

Links	https://issues.asterisk.org/jira/browse/ASTERISK-27382 https://issues.asterisk.org/jira/browse/ASTERISK-27429

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2017-012.pdf and http://downloads.digium.com/pub/security/AST-2017-012.html

Revision History		
Date	**Editor**	**Revisions Made**

November 30, 2017	Joshua Colp	Initial Revision