Product	Asterisk
Summary	RTP/RTCP information leak
Nature of Advisory	Unauthorized data disclosure
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	Yes
Reported On	September 1, 2017
Reported By	Klaus-Peter Junghanns
Posted On	September 19, 2017
Last Updated On	September 20, 2017
Advisory Contact	Richard Mudgett <rmudgett AT digium DOT com>
CVE Name	CVE-2017-14099, CVE-2017-14603

Description	This is a follow up advisory to AST-2017-005. Insufficient RTCP packet validation could allow reading stale buffer contents and when combined with the “nat” and “symmetric_rtp” options allow redirecting where Asterisk sends the next RTCP report. The RTP stream qualification to learn the source address of media always accepted the first RTP packet as the new source and allowed what AST-2017-005 was mitigating. The intent was to qualify a series of packets before accepting the new source address.

Resolution	The RTP/RTCP stack will now validate RTCP packets before processing them. Packets failing validation are discarded. RTP stream qualification now requires the intended series of packets from the same address without seeing packets from a different source address to accept a new source address.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	11.x	All Releases
Asterisk Open Source	13.x	All Releases
Asterisk Open Source	14.x	All Releases
Certified Asterisk	11.6	All Releases
Certified Asterisk	13.13	All Releases

Corrected In	
Product	**Release**
Asterisk Open Source	11.25.3, 13.17.2, 14.6.2
Certified Asterisk	11.6-cert18, 13.13-cert6

Patches	
SVN URL	**Revision**
`http://downloads.asterisk.org/pub/security/AST-2017-008-11.diff`	Asterisk 11
`http://downloads.asterisk.org/pub/security/AST-2017-008-13.diff`	Asterisk 13
`http://downloads.asterisk.org/pub/security/AST-2017-008-14.diff`	Asterisk 14
`http://downloads.asterisk.org/pub/security/AST-2017-008-11.6.diff`	Certified Asterisk 11.6
`http://downloads.asterisk.org/pub/security/AST-2017-008-13.13.diff`	Certified Asterisk 13.13

Links	https://issues.asterisk.org/jira/browse/ASTERISK-27274 https://issues.asterisk.org/jira/browse/ASTERISK-27252

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2017-008.pdf and

http://downloads.digium.com/pub/security/AST-2017-008.html

Revision History		
Date	**Editor**	**Revisions Made**
09/15/2017	Richard Mudgett	Initial revision
09/19/2017	Joshua Colp	Added CVE
09/20/2017	Joshua Colp	Added CVE for RTCP