Product	Asterisk
Summary	Media takeover in RTP stack
Nature of Advisory	Unauthorized data disclosure
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	May 17, 2017
Reported By	Klaus-Peter Junghanns
Posted On	August 31, 2017
Last Updated On	August 31, 2017
Advisory Contact	Joshua Colp <jcolp AT digium DOT com>
CVE Name	CVE-2017-14099

Description	The “strictrtp” option in rtp.conf enables a feature of the RTP stack that learns the source address of media for a session and drops any packets that do not originate from the expected address. This option is enabled by default in Asterisk 11 and above. The “nat” and “rtp_symmetric” options for chan_sip and chan_pjsip respectively enable symmetric RTP support in the RTP stack. This uses the source address of incoming media as the target address of any sent media. This option is not enabled by default but is commonly enabled to handle devices behind NAT. A change was made to the strict RTP support in the RTP stack to better tolerate late media when a reinvite occurs. When combined with the symmetric RTP support this introduced an avenue where media could be hijacked. Instead of only learning a new address when expected the new code allowed a new source address to be learned at all times. If a flood of RTP traffic was received the strict RTP support would allow the new address to provide media and with symmetric RTP enabled outgoing traffic would be sent to this new address, allowing the media to be hijacked. Provided the attacker continued to send traffic they would continue to receive traffic as well.

Resolution	The RTP stack will now only learn a new source address if it has been told to expect the address to change. The RTCP support has now also been updated to drop RTCP reports that are not regarding the RTP session currently in progress. The strict RTP learning progress has also been improved to guard against a flood of RTP packets attempting to take over the media stream.

Affected Versions

Product	Release Series	
Asterisk Open Source	11.x	11.4.0
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	11.25.2, 13.17.1, 14.6.1
Certified Asterisk	11.6-cert17, 13.13-cert5

Patches

SVN URL	Revision
http://downloads.asterisk.org/pub/security/AST-2017-005-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2017-005-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2017-005-14.diff	Asterisk 14
http://downloads.asterisk.org/pub/security/AST-2017-005-11.6.diff	Certified Asterisk 11.6
http://downloads.asterisk.org/pub/security/AST-2017-005-13.13.diff	Certified Asterisk 13.13

Links	https://issues.asterisk.org/jira/browse/ASTERISK-27013

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-2017-005.pdf and http://downloads.digium.com/pub/security/AST-2017-005.html

Revision History		
Date	**Editor**	**Revisions Made**
May 30, 2017	Joshua Colp	Initial Revision
August 31, 2017	Kevin Harwell	Updated for CVE