Product	Asterisk
Summary	RTP Resource Exhaustion
Nature of Advisory	Denial of Service
Susceptibility	Remote Authenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	August 5, 2016
Reported By	Etienne Lessard
Posted On	
Last Updated On	October 25, 2016
Advisory Contact	Joshua Colp <jcolp AT digium DOT com>
CVE Name	

Description	The overlap dialing feature in chan_sip allows chan_sip to report to a device that the number that has been dialed is incomplete and more digits are required. If this functionality is used with a device that has performed username/password authentication RTP resources are leaked. This occurs because the code fails to release the old RTP resources before allocating new ones in this scenario. If all resources are used then RTP port exhaustion will occur and no RTP sessions are able to be set up. UPDATE (20 October, 2016): It has been brought to our attention by Walter Doekes that this same leak can be exploited without the use of the overlap dialing feature. Sending SIP requests in a specific sequence outside the norm could also cause the leak of RTP resources. By sending an in-dialog INVITE after receiving a 404 response (but before sending an ACK), an attacker could cause the same leak to occur.

Resolution	If overlap dialing support is not needed the “allowoverlap” option can be set to no. This will stop any usage of the scenario which causes the resource exhaustion. If overlap dialing support is needed a change has been made so that existing RTP resources are destroyed in this scenario before allocating new resources. UPDATE (20 October, 2016): Because of the updated information from Walter Doekes, disabling the allowoverlap option is not enough to solve this issue. Users of Asterisk MUST upgrade to one of the fixed versions listed below.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	11.x	All Versions
Asterisk Open Source	13.x	All Versions
Certified Asterisk	11.6	All Versions
Certified Asterisk	13.8	All Versions

Corrected In	
Product	**Release**
Asterisk Open Source	11.23.1, 13.11.1
Certified Asterisk	11.6-cert15, 13.8-cert3

Patches	
SVN URL	**Revision**

Links	https://issues.asterisk.org/jira/browse/ASTERISK-26272

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2016-007.pdf and http://downloads.digium.com/pub/security/AST-2016-007.html

Revision History		
Date	**Editor**	**Revisions Made**
August 23, 2016	Joshua Colp	Initial creation
October 20, 2016	Mark Michelson	Added updates to the description and resolution.