Product	Asterisk
Summary	Remote Crash when Invalid SDP is sent in SIP Request
Nature of Advisory	Remote Crash
Susceptibility	Remote Unauthenticated Sessions
Severity	Major
Exploits Known	None
Reported On	July 03, 2013
Reported By	Walter Doekes, OSSO B.V.
Posted On	August 27, 2013
Last Updated On	August 28, 2013
Advisory Contact	Matthew Jordan <mjordan AT digium DOT com>
CVE Name	CVE-2013-5642

Description	A remotely exploitable crash vulnerability exists in the SIP channel driver if an invalid SDP is sent in a SIP request that defines media descriptions before connection information. The handling code incorrectly attempts to reference the socket address information even though that information has not yet been set.

Resolution	This patch adds checks when handling the various media descriptions that ensures the media descriptions are handled only if we have connection information suitable for that media. Thanks to Walter Doekes of OSSO B.V. for finding, reporting, testing, and providing the fix for this problem.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	All Versions
Asterisk Open Source	10.x	All Versions
Asterisk Open Source	11.x	All Versions
Certified Asterisk	1.8.15	All Versions
Certified Asterisk	11.2	All Versions
Asterisk with Digiumphones	10.x-digiumphones	All Versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.23.1, 10.12.3, 11.5.1
Certified Asterisk	1.8.15-cert3, 11.2-cert2
Asterisk with Digiumphones	10.12.3-digiumphones

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2013-005-1.8.diff	Asterisk 1.8
http://downloads.asterisk.org/pub/security/AST-2013-005-10.diff	Asterisk 10
http://downloads.asterisk.org/pub/security/AST-2013-005-10-digiumphones.diff	Asterisk 10-digiumphones
http://downloads.asterisk.org/pub/security/AST-2013-005-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2013-005-1.8.15.diff	Certified Asterisk 1.8.15
http://downloads.asterisk.org/pub/security/AST-2013-005-11.2.diff	Certified Asterisk 11.2

Links	https://issues.asterisk.org/jira/browse/ASTERISK-22007

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2013-005.pdf and http://downloads.digium.com/pub/security/AST-2013-005.html

Revision History		
Date	**Editor**	**Revisions Made**
2013-08-27	Matt Jordan	Initial Revision.
2013-08-28	Matt Jordan	Updated CVE.