Product	Asterisk
Summary	Remote Crash From Late Arriving SIP ACK With SDP
Nature of Advisory	Remote Crash
Susceptibility	Remote Unauthenticated Sessions
Severity	Major
Exploits Known	None
Reported On	February 11, 2013
Reported By	Colin Cuthbertson
Posted On	August 27, 2013
Last Updated On	August 28, 2013
Advisory Contact	Joshua Colp <jcolp AT digium DOT com>
CVE Name	CVE-2013-5641

Description	A remotely exploitable crash vulnerability exists in the SIP channel driver if an ACK with SDP is received after the channel has been terminated. The handling code incorrectly assumes that the channel will always be present.

Resolution	A check has now been added which only parses SDP and applies it if an Asterisk channel is present.
	Note that Walter Doekes, OSSO B.V., is responsible for diagnosing and providing the fix for this issue.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	1.8.17.0 and above
Asterisk Open Source	11.x	All versions
Certified Asterisk	1.8.15	All versions
Certified Asterisk	11.2	All versions

Corrected In

Product	Release
Asterisk Open Source	1.8.23.1, 11.5.1
Certified Asterisk	1.8.15-cert3, 11.2-cert2

Patches

SVN URL	Revision
http://downloads.asterisk.org/pub/security/ AST-2013-004-1.8.diff	Asterisk 1.8
http://downloads.asterisk.org/pub/security/ AST-2013-004-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/ AST-2013-004-1.8.15-cert.diff	Certified Asterisk 1.8.15
http://downloads.asterisk.org/pub/security/ AST-2013-004-11.2-cert.diff	Certified Asterisk 11.1

Links	https://issues.asterisk.org/jira/browse/ASTERISK-21064

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2013-004.pdf and http://downloads.digium.com/pub/security/AST-2013-004.html

Revision History

Date	Editor	Revisions Made
2013-08-22	Joshua Colp	Initial revision.
2013-08-28	Matt Jordan	Updated with CVE.