Product	Asterisk
Summary	Buffer Overflow when receiving odd length 16 bit SMS message
Nature of Advisory	Buffer Overflow and Remote Crash
Susceptibility	Remote SMS Messages
Severity	Major
Exploits Known	None
Reported On	September 26, 2013
Reported By	Jan Juergens
Posted On	December 16, 2013
Last Updated On	December 17, 2013
Advisory Contact	Scott Griepentrog <sgriepentrog AT digium DOT com>
CVE Name	CVE-2013-7100

Description	A 16 bit SMS message that contains an odd message length value will cause the message decoding loop to run forever. The message buffer is not on the stack but will be overflowed resulting in corrupted memory and an immediate crash.

Resolution	This patch corrects the evaluation of the message length indicator, ensuring that the message decoding loop will stop at the end of the received message. Thanks to Jan Juergens for finding, reporting, testing, and providing a 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 with Digiumphones	10.x-digiumphones	All Versions
Asterisk Open Source	11.x	All Versions
Certified Asterisk	1.8.x	All Versions
Certified Asterisk	11.x	All Versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.24.1, 10.12.4, 11.6.1
Asterisk with Digiumphones	10.12.4-digiumphones
Certified Asterisk	1.8.15-cert4, 11.2-cert3

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2013-006-1.8.diff	Asterisk 1.8
http://downloads.asterisk.org/pub/security/AST-2013-006-10.diff	Asterisk 10
http://downloads.asterisk.org/pub/security/AST-2013-006-10-digiumphones.diff	Asterisk 10-digiumphones
http://downloads.asterisk.org/pub/security/AST-2013-006-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2013-006-1.8.15.diff	Certified Asterisk 1.8.15
http://downloads.asterisk.org/pub/security/AST-2013-006-11.2.diff	Certified Asterisk 11.2

Links	https://issues.asterisk.org/jira/browse/ASTERISK-22590

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2013-006.pdf and http://downloads.digium.com/pub/security/AST-2013-006.html

Revision History		
Date	**Editor**	**Revisions Made**
12/16/2013	Scott Griepentrog	Initial Revision
12/17/2013	Matt Jordan	Updated CVE