Product	Asterisk
Summary	Heap Buffer Overflow in Skinny Channel Driver
Nature of Advisory	Exploitable Heap Buffer Overflow
Susceptibility	Remote Authenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	March 26, 2012
Reported By	Russell Bryant
Posted On	April 23, 2012
Last Updated On	April 23, 2012
Advisory Contact	Matt Jordan < mjordan AT digium DOT com >
CVE Name	CVE-2012-2415

Description	In the Skinny channel driver, KEYPAD_BUTTON_MESSAGE events are queued for processing in a buffer allocated on the heap, where each DTMF value that is received is placed on the end of the buffer. Since the length of the buffer is never checked, an attacker could send sufficient KEYPAD_BUTTON_MESSAGE events such that the buffer is overrun.

Resolution	The length of the buffer is now checked before appending a value to the end of the buffer.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.6.2.x	All Versions
Asterisk Open Source	1.8.x	All Versions
Asterisk Open Source	10.x	All Versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.6.2.24, 1.8.11.1, 10.3.1

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2012-005-1.6.2.diff	v1.6.2
http://downloads.asterisk.org/pub/security/AST-2012-005-1.8.diff	v1.8
http://downloads.asterisk.org/pub/security/AST-2012-005-10.diff	v10

Links	https://issues.asterisk.org/jira/browse/ASTERISK-19592

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2012-005.pdf and http://downloads.digium.com/pub/security/AST-2012-005.html

Revision History		
Date	**Editor**	**Revisions Made**
04/16/2012	Matt Jordan	Initial Release
04/23/2012	Matt Jordan	Added CVE Number