Product	Asterisk
Summary	Remote crash vulnerability in Skinny channel driver
Nature of Advisory	Denial of Service
Susceptibility	Remote Authenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	August 7, 2007
Reported By	Wei Wang of McAfee AVERT Labs
Posted On	August 7, 2007
Last Updated On	August 21, 2007
Advisory Contact	Jason Parker <jparker@digium.com>
CVE Name	CVE-2007-4280

Description	The Asterisk Skinny channel driver, chan_skinny, has a remotely exploitable crash vulnerability. A segfault can occur when Asterisk receives a "CAPABILITIES_RES_MESSAGE" packet where the capabilities count is greater than the total number of items in the capabilities_res_message array. Note that this requires an authenticated session.

Resolution	Asterisk code has been modified to limit the incoming capabilities count. Users with configured Skinny devices should upgrade to the appropriate version listed in the corrected in section of this advisory.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.0.x	Not affected
Asterisk Open Source	1.2.x	Not affected
Asterisk Open Source	1.4.x	All versions prior to 1.4.10
Asterisk Business Edition	A.x.x	Not affected
Asterisk Business Edition	B.x.x	Not affected
AsteriskNOW	pre-release	All versions prior to beta7
Asterisk Appliance Developer Kit	0.x.x	All versions prior to 0.7.0
s800i (Asterisk Appliance)	1.0.x	All versions prior to 1.0.3

Corrected In	
Product	**Release**
Asterisk Open Source	1.4.10, available from http://downloads.digium.com/pub/telephony/asterisk
AsteriskNOW	Beta7, available from http://www.asterisknow.org/. Beta5 and Beta6 users can update using the system update feature in the appliance control panel.
Asterisk Appliance Developer Kit	0.7.0, available from http://downloads.digium.com/pub/telephony/aadk
s800i (Asterisk Appliance)	1.0.3

Links	

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/asa/AST-2007-019.pdf and http://downloads.digium.com/pub/asa/AST-2007-019.html.

Revision History		
Date	**Editor**	**Revisions Made**
August 7, 2007	jparker@digium.com	Initial Release
August 9, 2007	jparker@digium.com	Added CVE Name
August 21, 2007	russell@digium.com	Changed name prefix from ASA to AST