Product	Asterisk
Summary	Remote Crash Vulnerability in IAX2 channel driver
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	July 13, 2007
Reported By	Chris Clark and Zane Lackey, iSEC Partners
Posted On	July 17, 2007
Last Updated On	August 21, 2007
Advisory Contact	Russell Bryant <russell@digium.com>
CVE Name	CVE-2007-3763

Description	The Asterisk IAX2 channel driver, chan_iax2, has a remotely exploitable crash vulnerability. A NULL pointer exception can occur when Asterisk receives a LAGRQ or LAGRP frame that is part of a valid session and includes information elements. The session used to exploit this issue does not have to be authenticated. It can simply be a NEW packet sent with an invalid username. The code that parses the incoming frame correctly parses the information elements of IAX frames. It then sets a pointer to NULL to indicate that there is not a raw data payload associated with this frame. However, it does not set the variable that indicates the number of bytes in the raw payload back to zero. Since the raw data length is non-zero, the code handling LAGRQ and LAGRP frames tries to copy data from a NULL pointer, causing a crash.

Resolution	All users that have chan_iax2 enabled 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	All versions
Asterisk Open Source	1.2.x	All versions prior to 1.2.22
Asterisk Open Source	1.4.x	All versions prior to 1.4.8
Asterisk Business Edition	A.x.x	All versions
Asterisk Business Edition	B.x.x	All versions prior to B.2.2.1
AsteriskNOW	pre-release	All versions prior to beta7
Asterisk Appliance Developer Kit	0.x.x	All versions prior to 0.5.0
s800i (Asterisk Appliance)	1.0.x	All versions prior to 1.0.2

Corrected In	
Product	**Release**
Asterisk Open Source	1.2.22 and 1.4.8, available from http://downloads.digium.com/pub/telephony/asterisk
Asterisk Business Edition	B.2.2.1, available from the Asterisk Business Edition user portal on http://www.digium.com or via Digium Technical Support
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	0.5.0, available from http://downloads.digium.com/pub/telephony/aadk/
s800i (Asterisk Appliance)	1.0.2

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-2007-015.pdf and http://downloads.digium.com/pub/asa/AST-2007-015.html.

Revision History

Date	Editor	Revisions Made
July 17, 2007	russell@digium.com	Initial Release
August 21, 2007	russell@digium.com	Changed name prefix from ASA to AST, changed ftp.digium.com to downloads.digium.com