Product	Asterisk
Summary	Stack buffer overflow in IAX2 channel driver
Nature of Advisory	Exploitable Stack Buffer Overflow
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	July 12, 2007
Reported By	Russell Bryant, Digium, Inc.
Posted On	July 17, 2007
Last Updated On	August 21, 2007
Advisory Contact	Russell Bryant <russell@digium.com>
CVE Name	CVE-2007-3762

Description	The Asterisk IAX2 channel driver, chan_iax2, has a remotely exploitable stack buffer overflow vulnerability. It occurs when chan_iax2 is passed a voice or video frame with a data payload larger than 4 kB. This is exploitable by sending a very large RTP frame to an active RTP port number used by Asterisk when the other end of the call is an IAX2 channel. Exploiting this issue can cause a crash or allow arbitrary code execution on a remote machine. The specific conditions that trigger the vulnerability are the following: ● iax2_write() is called with a frame with the following properties ○ a voice or video frame ○ Its 4-byte timestamp has the same high 2 bytes as the previous frame that was sent ○ Its format is the one currently expected ○ Its data payload is larger than 4 kB iax2_write() calls iax2_send() to send the frame. Inside of iax2_send(), there is a conditional check to determine whether the frame should be sent immediately (the now variable) or queued for transmission later. If the frame is going to be transmitted later, an iax_frame struct is dynamically allocated with a data buffer that has the exact buffer size needed to accommodate for the provided ast_frame data. However, if the frame is being sent immediately, it uses a stack allocated iax_frame, with a data buffer size of 4096 bytes. Later, the iax_frame_wrap() function is used to copy the data from the ast_frame struct into the iax_frame struct. This function assumes the iax_frame data buffer has enough space for all of the data in the ast_frame.

Resolution	This issue is only exploitable when the system is configured in such a way that calls between channels that use RTP and IAX2 channels are possible. Also, some additional protection against arbitrary code execution is provided if the call involves transcoding between audio formats as this will change the contents of the frame payload. All users that have systems that connect calls between channels that use RTP and IAX2 channels should immediately update to versions 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-2007-014.pdf and http://downloads.digium.com/pub/asa/AST-2007-014.html.

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