Product	Asterisk
Summary	IAX2 users can cause unauthorized data disdosure
Nature of Advisory	Unauthorized information disclosure
Susceptibility	Remote authenticated sessions
Severity	Low
Exploits Known	No
Reported On	April 27, 2007
Reported By	Tim Panton, Mexuar, <tim@mexuar.com> Birgit Arkesteijn, Westhawk, <birgit@westhawk.co.uk>
Posted On	May 4, 2007
Last Updated On	August 21, 2007
Advisory Contact	kpfleming@digium.com
CVE Name	CVE-2007-2488

Description	> From: Tim Panton <tim@mexuar.com> > Date: 27 April 2007 08:02:36 BDT > To: "Kevin P. Fleming" <kpfleming@digium.com> > Subject: Possible IAX2 vulnerability (Minor) > > We've stumbled on a bug in the way Asterisk's IAX2 handles text > frames. > I'm emailing you because it is a borderline security vulnerability, > and my > friends in the security world tell me that I should notify the > vendor privately > first. If you feel it isn't a security issue, let me know and I'll > put it in mantis. > > chan_iax2 assumes that the content of a text frame is a null > terminated > string (C style), and when time comes to forward the string it uses > strlen > to determine the message length. > > If you send a frame without a 0 byte in it, Asterisk forwards a > frame that > includes the sent data and some extra (presumably heap) data. > > If an attacker were lucky, the extra data could contain something > interesting. > Or conceivably it could cause a segmentation violation.

Resolution	Asterisk code has been modified to enforce null-termination of incoming text frames received by the IAX2 channel driver (chan_iax2). When text frames are received without null-termination, this may result in the last byte of data in the frame being lost, if the IAX2 reception process does not have space in its receive buffer to add a null character. As this vulnerability is of 'low' severity, it does not justify new releases of Asterisk solely for mitigating its impact. The fix for this vulnerability has been committed to the Asterisk Subversion source code repositories and is available to all users who wish to upgrade to a prerelease checkout of the respective development branch for their release series of Asterisk. All other users can upgrade when the next regularly scheduled release of their product is produced.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.0.x	has not been evaluated as this release series is no longer maintained
Asterisk Open Source	1.2.x	all releases prior to 1.2.19
Asterisk Open Source	1.4.x	all releases prior to 1.4.5
Asterisk Business Edition	A.x.x	all releases
Asterisk Business Edition	B.x.x	all releases prior to B.2.1
AsteriskNOW	pre-release	all releases prior to and including Beta 5
Asterisk Appliance Developer Kit	0.x.x	all releases prior to 0.4.1

Corrected In	
Product	**Release**
Asterisk Open Source	1.2.19 and 1.4.5 will be available from http://http.digium.com/pub/telephony/asterisk when released
Asterisk Business Edition	B.2.1, will be available from the Asterisk Business Edition user portal on http://www.digium.com or via Digium Technical Support when released
AsteriskNOW	Beta 6, when available from http://www.asterisknow.org, Beta 5 users can use 'System Update' in the appliance control panel to update their version of AsteriskNOW when Asterisk 1.4.4 has been released
Asterisk Appliance Developer Kit	0.4.1, will be available from http://downloads.digium.com/pub/telephony/aadk when released

Links	http://bugs.digium.com/view.php?id=9638

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-2007-013.pdf.

Revision History		
Date	**Editor**	**Revisions Made**
May 4, 2007	kpfleming@digium.com	initial release
May 4, 2007	kpfleming@digium.com	proper 'corrected in' release number for Asterisk 1.4
August 21, 2007	russell@digium.com	Changed name prefix from ASA to AST