Asterisk Project Security Advisory - AST-2008-006

Product	Asterisk
Summary	3-way handshake in IAX2 incomplete
Nature of Advisory	Remote amplification attack
Susceptibility	Remote unauthenticated sessions
Severity	Critical
Exploits Known	Yes
Reported On	April 18, 2008
Reported By	Joel R. Voss aka. Javantea < jvoss AT altsci DOT com >
Posted On	April 22, 2008
Last Updated On	December 12, 2008
Advisory Contact	Tilghman Lesher < tlesher AT digium DOT com >
CVE Name	CVE-2008-1897

Description	Javantea originally reported an issue in IAX2, whereby an attacker could send a spoofed IAX2 NEW message, and Asterisk would start sending early audio to the target address, without ever receiving an initial response. That original vulnerability was addressed in June 2007, by requiring a response to the initial NEW message before starting to send any audio. Javantea subsequently found that we were doing insufficent verification of the ACK response and that the ACK response could be spoofed, just like the initial NEW message. We have addressed this failure with two changes. First, we have started to require that the ACK response contains the unique source call number that we send in our reply to the NEW message. Any ACK response that does not contain the source call number that we have created will be silently thrown away. Second, we have made the generation of our source call number a little more difficult to predict, by randomly selecting a source call number, instead of allocating them sequentially.

Workaround	Disable remote unauthenticated IAX2 sessions, by disallowing guest access.

Resolution	Upgrade your Asterisk installation to revision 114561 or later, or install one of the releases shown below.

Commentary	We would like to thank Javantea for notifying us of this problem; however, we note that he posted exploit code prior to that notification, which is considered irresponsible behavior in the whitehat security industry. In the future, advance notice of any such release would be appreciated.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.0.x	All versions
Asterisk Open Source	1.2.x	All versions prior to 1.2.28
Asterisk Open Source	1.4.x	All versions prior to 1.4.19.1
Asterisk Business Edition	A.x.x	All versions
Asterisk Business Edition	B.x.x	All versions prior to B.2.5.2
Asterisk Business Edition	C.x.x	All versions prior to C.1.8.1
AsteriskNOW	1.0.x	All versions prior to 1.0.3
Asterisk Appliance Developer Kit	0.x.x	All versions
s800i (Asterisk Appliance)	1.0.x	All versions prior to 1.1.0.3

Corrected In	
Product	**Release**
Asterisk Open Source	1.2.28
Asterisk Open Source	1.4.19.1
Asterisk Business Edition	B.2.5.2
Asterisk Business Edition	C.1.8.1
AsteriskNOW	1.0.3
s800i (Asterisk Appliance)	1.1.0.3

Patches	
URL	**Version**
http://downloads.digium.com/pub/security/AST-2008-006-1.2.patch	1.2
http://downloads.digium.com/pub/security/AST-2008-006-1.4.patch	1.4

Links	https://www.altsci.com/concepts/page.php?s=asteri&p=2

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-2008-006.pdf and

http://downloads.digium.com/pub/security/AST-2008-006.html

Revision History		
Date	**Editor**	**Revisions Made**
April 22, 2008	Tilghman Lesher	Initial release
April 22, 2008	Tilghman Lesher	Corrected 1.4 version where fix was released.
December 12, 2008	Tilghman Lesher	Added patches