Product	Asterisk
Summary	Remote Crash Vulnerability in STUN implementation
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	July 13, 2007
Reported By	Will Drewry, Google Security Team
Posted On	July 17, 2007
Last Updated On	August 21, 2007
Advisory Contact	Joshua Colp <jcolp@digium.com>
CVE Name	CVE-2007-3765

Description	The Asterisk STUN implementation in the RTP stack has a remotely exploitable crash vulnerability. A pointer may run past accessible memory if Asterisk receives a specially crafted STUN packet on an active RTP port. The code that parses the incoming STUN packets incorrectly checks that the length indicated in the STUN attribute and the size of the STUN attribute header does not exceed the available data. This will cause the data pointer to run past accessible memory and when accessed will cause a crash.

Resolution	All users that have chan_sip, chan_gtalk, chan_jingle, chan_h323, chan_mgcp, or chan_skinny enabled on an affected version should upgrade to the appropriate version listed in the correct in section of this advisory.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.0.x	None affected
Asterisk Open Source	1.2.x	None affected
Asterisk Open Source	1.4.x	All versions prior to 1.4.8
Asterisk Business Edition	A.x.x	None affected
Asterisk Business Edition	B.x.x	None affected
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	1.4.8 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	0.5.0, 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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/asa/AST-2007-017.pdf and http://downloads.digium.com/pub/asa/AST-2007-017.html.

Revision History		
Date	**Editor**	**Revisions Made**
July 17, 2006	jcolp@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