Product	Asterisk
Summary	Remote Crash Vulnerability in SIP channel driver
Nature of Advisory	Remote attacker can crash an Asterisk server
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	Yes
Reported On	06/13/2011
Reported By	jaredmauch
Posted On	06/23/2011
Last Updated On	June 23, 2011
Advisory Contact	Paul Belanger pabelanger@digium.com
CVE Name	CVE Requested

Description	A remote user sending a SIP packet containing a Contact header with a missing left angle bracket (<) causes Asterisk to access a null pointer.

Resolution	Asterisk now warns the user of the missing bracket and continues processing. Available workarounds are to disable chan_sip or to upgrade.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	All

Corrected In	
Product	**Release**
Asterisk Open Source 1.8.x	1.8.4.3

Patches	
SVN URL	**Revision**
Http://downloads.asterisk.org/pub/security/AST-2011-009.diff	1.8

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This document may be superseded by later versions; if so, the latest version will be posted at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-2011-009.pdf and
http://downloads.digium.com/pub/security/AST-2011-009.html

Revision History		
Date	**Editor**	**Revisions Made**
06/20/2011	Kinsey Moore	Initial Release