Product	Asterisk
Summary	Remote Crash Vulnerability in SIP channel driver
Nature of Advisory	Remote attacker can crash an Asterisk server
Susceptibility	Remote Authenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	05/23/11
Reported By	Jonathan Rose jrose@digium.com
Posted On	06/02/11
Last Updated On	06/02/11
Advisory Contact	Jonathan Rose jrose@digium.com
CVE Name	CVE-2011-2216

Description	If a remote user initiates a SIP call and the recipient picks up, the remote user can reply with a malformed Contact header that Asterisk will improperly handle and cause a crash due to a segmentation fault.

Resolution	Asterisk now immediately initializes buffer strings coming into the parse_uri_full function to prevent outside functions from receiving a NULL value pointer. This should increase the safety of any function that uses parse_uri or its wrapper functions which previously would attempt to work in the presence of a parse_uri failure by reading off of potentially uninitialized strings.

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

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.4.2

Patches	
URL	**Branch**
Http://downloads.asterisk.org/pub/security/AST-2011-007-1.8.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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2011-007.pdf and http://downloads.digium.com/pub/security/AST-2011-007.html

Revision History		
Date	**Editor**	**Revisions Made**
06/02/11	Jonathan Rose	Initial Release