Product	Asterisk
Summary	Remote crash possibility with SIP and the “automon” feature enabled
Nature of Advisory	Remote crash vulnerability in a feature that is disabled by default
Susceptibility	Remote unauthenticated sessions
Severity	Moderate
Exploits Known	Yes
Reported On	November 2, 2011
Reported By	Kristijan Vrban
Posted On	2011-11-03
Last Updated On	December 7, 2011
Advisory Contact	Terry Wilson <twilson@digium.com>
CVE Name	

Description	When the “automon” feature is enabled in features.conf, it is possible to send a sequence of SIP requests that cause Asterisk to dereference a NULL pointer and crash.

Resolution	Applying the referenced patches that check that the pointer is not NULL before accessing it will resolve the issue. The “automon” feature can be disabled in features.conf as a workaround.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.6.2.x	All versions
Asterisk Open Source	1.8.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.6.2.21, 1.8.7.2

Patches	
Download URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2011-014-1.6.2.diff	1.6.2.20
http://downloads.asterisk.org/pub/security/AST-2011-014-1.8.diff	1.8.7.1

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This document may be superseded by later versions; if so, the latest version will be posted at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/security/AST-2011-014.pdf and
http://downloads.digium.com/pub/security/AST-2011-014.html

Revision History		
Date	**Editor**	**Revisions Made**