Product	Asterisk
Summary	Remote Crash Vulnerability in SIP Channel Driver
Nature of Advisory	Remote Crash
Susceptibility	Remote Authenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	April 16, 2012
Reported By	Thomas Arimont
Posted On	April 23, 2012
Last Updated On	April 23, 2012
Advisory Contact	Matt Jordan < mjordan AT digium DOT com >
CVE Name	CVE-2012-2416

Description	A remotely exploitable crash vulnerability exists in the SIP channel driver if a SIP UPDATE request is processed within a particular window of time. For this to occur, the following must take place: 1. The setting 'trustrpid' must be set to True 2. An UPDATE request must be received after a call has been terminated and the associated channel object has been destroyed, but before the SIP dialog associated with the call has been destroyed. Receiving the UPDATE request before the call is terminated or after the SIP dialog associated with the call will not cause the crash vulnerability described here. 3. The UPDATE request must be formatted with the appropriate headers to reflect an Asterisk connected line update. The information in the headers must reflect a different Caller ID then what was previously associated with the dialog. When these conditions are true, Asterisk will attempt to perform a connected line update with no associated channel, and will crash.

Resolution	Asterisk now ensures a channel exists before performing a connected line update, when that connected line update is initiated via a SIP UPDATE request. In Asterisk versions not containing the fix for this issue, setting the 'trustrpid' setting to False will prevent this crash from occurring (default is False)

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	All versions
Asterisk Open Source	10.x	All versions
Asterisk Business Edition	C.3.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.11.1, 10.3.1
Asterisk Business Edition	C.3.7.4

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2012-006-1.8.diff	v1.8
http://downloads.asterisk.org/pub/security/AST-2012-006-10.diff	v.10

Links	https://issues.asterisk.org/jira/browse/ASTERISK-19770

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2012-006.pdf and http://downloads.digium.com/pub/security/AST-2012-006.html

Revision History		
Date	**Editor**	**Revisions Made**
04/16/2012	Matt Jordan	Initial release.
04/23/2012	Matt Jordan	Added CVE Number.