Product	Asterisk
Summary	Skinny Channel Driver Remote Crash Vulnerability
Nature of Advisory	Denial of Service
Susceptibility	Remote authenticated sessions
Severity	Minor
Exploits Known	No
Reported On	May 30, 2012
Reported By	Christoph Hebeisen, TELUS Security Labs
Posted On	June 14, 2012
Last Updated On	June 14, 2012
Advisory Contact	Matt Jordan < mjordan AT digium DOT com >
CVE Name	CVE-2012-3553

Description	AST-2012-008 previously dealt with a denial of service attack exploitable in the Skinny channel driver that occurred when certain messages are sent after a previously registered station sends an Off Hook message. Unresolved in that patch is an issue in the Asterisk 10 releases, wherein, if a Station Key Pad Button Message is processed after an Off Hook message, the channel driver will inappropriately dereference a Null pointer. Similar to AST-2012-008, a remote attacker with a valid SCCP ID can can use this vulnerability by closing a connection to the Asterisk server when a station is in the “Off Hook” call state and crash the server.

Resolution	The presence of a device for a line is now checked in the appropriate channel callbacks, preventing the crash.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	10.x	All Versions

Corrected In	
Product	**Release**
Asterisk Open Source	10.5.1

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2012-009-10.diff	v10

Links	https://issues.asterisk.org/jira/browse/ASTERISK-19905

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2012-009.pdf and http://downloads.digium.com/pub/security/AST-2012-009.html

Revision History		
Date	**Editor**	**Revisions Made**
06/14/2012	Matt Jordan	Initial Release