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 22, 2012
Reported By	Christoph Hebeisen
Posted On	May 29, 2012
Last Updated On	May 29, 2012
Advisory Contact	Matt Jordan < mjordan AT digium DOT com >
CVE Name	CVE-2012-2948

Description	As reported by Telus Labs: "A Null-pointer dereference has been identified in the SCCP (Skinny) channel driver of Asterisk. When an SCCP client closes its connection to the server, a pointer in a structure is set to Null. If the client was not in the on-hook state at the time the connection was closed, this pointer is later dereferenced. A remote attacker with a valid SCCP ID can can use this vulnerability by closing a connection to the Asterisk server in certain call states (e.g. "Off hook") to crash the server. Successful exploitation of this vulnerability would result in termination of the server, causing denial of service to legitimate users."

Resolution	The pointer to the device in the structure is now checked before it is dereferenced in the channel event callbacks and message handling functions.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	All Versions
Asterisk Open Source	10.x	All Versions
Certified Asterisk	1.8.11-cert	1.8.11-cert1

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.12.1, 10.4.1
Certified Asterisk	1.8.11-cert2

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2012-008-1.8.diff	v1.8
http://downloads.asterisk.org/pub/security/AST-2012-008-10.diff	v10
http://downloads.asterisk.org/pub/security/AST-2012-008-1.8.11-cert.diff	v1.8.11-cert

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2012-008.pdf and http://downloads.digium.com/pub/security/AST-2012-008.html

Revision History		
Date	**Editor**	**Revisions Made**
05/25/2012	Matt Jordan	Initial Release