Asterisk Project Security Advisory - AST-2011-004

Product	Asterisk
Summary	Remote crash vulnerability in TCP/TLS server
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	March 1, 2011
Reported By	Blake Cornell <blake@remoteorigin.com> and Chris Maj <chris@penguinpbx.com>
Posted On	March 16, 2011
Last Updated On	March 14, 2011
Advisory Contact	Terry Wilson <twilson@digium.com>

Description	Rapidly opening and closing TCP connections to services using the ast_tcptls_* API (primarily chan_sip, manager, and res_phoneprov) can cause Asterisk to crash after dereferencing a NULL pointer.

Resolution	Failure of the fdopen call is detected and dereferencing the NULL pointer is avoided.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.6.1.x	All versions
Asterisk Open Source	1.6.2.x	All versions
Asterisk Open Source	1.8.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.6.1.23, 1.6.2.17.1, 1.8.3.1

Patches	
URL	**Branch**
http://downloads.asterisk.org/pub/security/AST-2011-004-1.6.1.diff	1.6.1
http://downloads.asterisk.org/pub/security/AST-2011-004-1.6.2.diff	1.6.2
http://downloads.asterisk.org/pub/security/AST-2011-004-1.8.diff	1.8

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2011-004.pdf and http://downloads.digium.com/pub/security/AST-2011-004.html

Revision History		
Date	**Editor**	**Revisions Made**
2011-03-14	Terry Wilson	Initial release