Product	Asterisk
Summary	Remote crash vulnerability in voice mail application
Nature of Advisory	Denial of Service
Susceptibility	Remote authenticated sessions
Severity	Moderate
Exploits Known	No
Reported On	June 13, 2012
Reported By	Nicolas Bouliane – Avencall Security Labs
Posted On	June 27, 2012
Last Updated On	July 5, 2012
Advisory Contact	Kinsey Moore <kmoore@digium.com>
CVE Name	CVE-2012-3812

Description	If a single voicemail account is manipulated by two parties simultaneously, a condition can occur where memory is freed twice causing a crash.

Resolution	Management of the memory in question has been reworked so that double frees and out of bounds array access do not occur. Upgrade to the latest release.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	1.8.11 and newer
Asterisk Open Source	10.x	10.3 and newer
Certified Asterisk	1.8.11-certx	All versions
Asterisk Digiumphones	10.x.x-digiumphones	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.13.1, 10.5.2
Certified Asterisk	1.8.11-cert4
Asterisk Digiumphones	10.5.2-digiumphones

Patches	
URL	**Revision**
http://downloads.asterisk.org/pub/security/ AST-2012-011-1.8.diff	Asterisk 1.8, Certified Asterisk
http://downloads.asterisk.org/pub/security/ AST-2012-011-10.diff	Asterisk 10, Asterisk Digiumphones

Links	https://issues.asterisk.org/jira/browse/ASTERISK-20052

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2012-011.pdf and http://downloads.digium.com/pub/security/AST-2012-011.html

Revision History		
Date	**Editor**	**Revisions Made**
06/27/2012	Kinsey Moore	Initial Release