Product	Asterisk
Summary	Cross-site AJAX request vulnerability
Nature of Advisory	Cross-site AJAX request exploitation
Susceptibility	Remote Unauthenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	October 26, 2009
Reported By	issues.asterisk.org user jcollie
Posted On	November 4, 2009
Last Updated On	November 4, 2009
Advisory Contact	Joshua Colp <jcolp AT digium DOT com>
CVE Name	CVE-2008-7220

Description	Asterisk includes a demonstration AJAX based manager interface, ajamdemo.html which uses the prototype.js framework. An issue was uncovered in this framework which could allow someone to execute a cross-site AJAX request exploit.

Resolution	Upgrade to one of the versions below, or apply one of the patches specified in the Patches section.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.2.x	Unaffected
Asterisk Open Source	1.4.x	All versions prior to 1.4.26.3
Asterisk Open Source	1.6.0.x	All versions prior to 1.6.0.17
Asterisk Open Source	1.6.1.x	All versions prior to 1.6.1.9
Asterisk Addons	1.2.x	Unaffected
Asterisk Addons	1.4.x	Unaffected
Asterisk Addons	1.6.x	Unaffected
Asterisk Business Edition	A.x.x	Unaffected
Asterisk Business Edition	B.x.x	All versions prior to B.2.5.12
Asterisk Business Edition	C.x.x	All versions prior to C.2.4.5 and C.3.2.2
AsteriskNOW	1.5	All versions
s800i (Asterisk Appliance)	1.2.x	Unaffected

Corrected In	
Product	**Release**
Asterisk Open Source	1.4.26.3
Asterisk Open Source	1.6.0.17
Asterisk Open Source	1.6.1.9
Asterisk Business Edition	B.2.5.12
Asterisk Business Edition	C.2.4.5
Asterisk Business Edition	C.3.2.2

Patches	
SVN URL	**Revision**
http://downloads.digium.com/pub/asa/AST-2009-009-1.4.diff.txt	1.4
http://downloads.digium.com/pub/asa/AST-2009-009-1.6.0.diff.txt	1.6.0
http://downloads.digium.com/pub/asa/AST-2009-009-1.6.1.diff.txt	1.6.1

Links	https://issues.asterisk.org/view.php?id=16139

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2009-009.pdf and http://downloads.digium.com/pub/security/AST-2009-009.html

Revision History		
Date	**Editor**	**Revisions Made**
October 29, 2009	Joshua Colp	Initial release