Product	Asterisk
Summary	Asterisk Manager User Unauthorized Shell Access
Nature of Advisory	Permission Escalation
Susceptibility	Remote Authenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	February 23, 2011
Reported By	David Woolley
Posted On	April 23, 2012
Last Updated On	April 23, 2012
Advisory Contact	Jonathan Rose < jrose AT digium DOT com >
CVE Name	CVE-2012-2414

Description	A user of the Asterisk Manager Interface can bypass a security check and execute shell commands when they lack permission to do so. Under normal conditions, a user should only be able to run shell commands if that user has System class authorization. Users could bypass this restriction by using the MixMonitor application with the originate action or by using either the GetVar or Status manager actions in combination with the SHELL and EVAL functions. The patch adds checks in each affected action to verify if a user has System class authorization. If the user does not have those authorizations, Asterisk rejects the action if it detects the use of any functions or applications that run system commands.

Resolution	Asterisk now performs checks against manager commands that cause these behaviors for each of the affected actions.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.6.2.x	All versions
Asterisk Open Source	1.8.x	All versions
Asterisk Open Source	10.x	All versions
Asterisk Business Edition	C.3.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.6.2.24, 1.8.11.1, 10.3.1
Asterisk Business Edition	C.3.7.4

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2012-004-1.6.2.diff	v1.6.2
http://downloads.asterisk.org/pub/security/AST-2012-004-1.8.diff	v1.8
http://downloads.asterisk.org/pub/security/AST-2012-004-10.diff	v10

Links	https://issues.asterisk.org/jira/browse/ASTERISK-17465

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2012-004.pdf and http://downloads.digium.com/pub/security/AST-2012-004.html

Revision History		
Date	**Editor**	**Revisions Made**
04/23/2012	Jonathan Rose	Initial Release
04/23/2012	Matt Jordan	Added CVE Number