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	April 9, 2014
Reported By	Corey Farrell
Posted On	June 12, 2014
Last Updated On	June 12, 2014
Advisory Contact	Jonathan Rose < jrose AT digium DOT com >
CVE Name	CVE-2014-4046

Description	Manager users can execute arbitrary shell commands with the MixMonitor manager action. Asterisk does not require system class authorization for a manager user to use the MixMonitor action, so any manager user who is permitted to use manager commands can potentially execute shell commands as the user executing the Asterisk process.

Resolution	Upgrade to a version with the patch integrated, apply the patch, or do not allow users who should not have permission to run shell commands to use AMI.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	11.x	All
Asterisk Open Source	12.x	All
Certified Asterisk	11.6	All

Corrected In	
Product	**Release**
Asterisk Open Source	11.10.1, 12.3.1
Certified Asterisk	11.6-cert3

Patches

SVN URL	Revision
http://downloads.asterisk.org/pub/security/ AST-2014-006-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/ AST-2014-006-12.diff	Asterisk 12
http://downloads.asterisk.org/pub/security/ AST-2014-006-11.6.diff	Certified Asterisk 11.6

Links	https://issues.asterisk.org/jira/browse/ASTERISK-23609

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2014-006.pdf and
http://downloads.digium.com/pub/security/AST-2014-006.html

Revision History

Date	Editor	Revisions Made
April 23, 2014	Jonathan Rose	Document Creation
June 12, 2014	Matt Jordan	Added CVE