Product	Asterisk
Summary	Asterisk Manager User Dialplan Permission Escalation
Nature of Advisory	Permission Escalation
Susceptibility	Remote Authenticated Sessions
Severity	Minor
Exploits Known	None
Reported On	November 25, 2013
Reported By	Matt Jordan
Posted On	December 16, 2013
Last Updated On	December 17, 2013
Advisory Contact	David Lee < dlee AT digium DOT com >
CVE Name	N/A

Description	External control protocols, such as the Asterisk Manager Interface, often have the ability to get and set channel variables; this allows the execution of dialplan functions. Dialplan functions within Asterisk are incredibly powerful, which is wonderful for building applications using Asterisk. But during the read or write execution, certain diaplan functions do much more. For example, reading the SHELL() function can execute arbitrary commands on the system Asterisk is running on. Writing to the FILE() function can change any file that Asterisk has write access to. When these functions are executed from an external protocol, that execution could result in a privilege escalation.

Resolution	Asterisk can now inhibit the execution of these functions from external interfaces such as AMI, if live_dangerously in the [options] section of asterisk.conf is set to no. For backwards compatibility, live_dangerously defaults to yes, and must be explicitly set to no to enable this privilege escalation protection.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	All Versions
Asterisk Open Source	10.x	All Versions
Asterisk with Digiumphones	10.x-digiumphones	All Versions
Asterisk Open Source	11.x	All Versions
Certified Asterisk	1.8.x	All Versions
Certified Asterisk	11.x	All Versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.24.1, 10.12.4, 11.6.1
Asterisk with Digiumphones	10.12.4-digiumphones
Certified Asterisk	1.8.15-cert4, 11.2-cert3

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2013-007-1.8.diff	Asterisk 1.8
http://downloads.asterisk.org/pub/security/AST-2013-007-10.diff	Asterisk 10
http://downloads.asterisk.org/pub/security/AST-2013-007-10-digiumphones.diff	Asterisk 10-digiumphones
http://downloads.asterisk.org/pub/security/AST-2013-007-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2013-007-1.8.15.diff	Certified Asterisk 1.8.15
http://downloads.asterisk.org/pub/security/AST-2013-007-11.2.diff	Certified Asterisk 11.2

Links	https://issues.asterisk.org/jira/browse/ASTERISK-22905

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-2013-007.pdf and http://downloads.digium.com/pub/security/AST-2013-007.html

Revision History		
Date	**Editor**	**Revisions Made**
12/16/2013	Matt Jordan	Initial Revision
12/17/2013	Matt Jordan	Updated CVE to N/A. Per guidelines from Mitre, a new security feature does not necessitate a CVE number.