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	July 13, 2012
Reported By	Zubair Ashraf of IBM X-Force Research
Posted On	August 30, 2012
Last Updated On	August 30, 2012
Advisory Contact	Matt Jordan < mjordan AT digium DOT com >
CVE Name	CVE-2012-2186

Description	The AMI Originate action can allow a remote user to specify information that can be used to execute shell commands on the system hosting Asterisk. This can result in an unwanted escalation of permissions, as the Originate action, which requires the “originate” class authorization, can be used to perform actions that would typically require the “system” class authorization. Previous attempts to prevent this permission escalation (AST-2011-006, AST-2012-004) have sought to do so by inspecting the names of applications and functions passed in with the Originate action and, if those applications/functions matched a predefined set of values, rejecting the command if the user lacked the “system” class authorization. As reported by IBM X-Force Research, the “ExternalIVR” application is not listed in the predefined set of values. The solution for this particular vulnerability is to include the “ExternalIVR” application in the set of defined applications/functions that require “system” class authorization. Unfortunately, the approach of inspecting fields in the Originate action against known applications/functions has a significant flaw. The predefined set of values can be bypassed by creative use of the Originate action or by certain dialplan configurations, which is beyond the ability of Asterisk to analyze at run-time. Attempting to work around these scenarios would result in severely restricting the applications or functions and prevent their usage for legitimate means. As such, any additional security vulnerabilities, where an application/function that would normally require the “system” class authorization can be executed by users with the “originate” class authorization, will not be addressed. Instead, the README-SERIOUSLY.bestpractices.txt file has been updated to reflect that the AMI Originate action can result in commands requiring the “system” class authorization to be executed. Proper system configuration can limit the impact of such scenarios.

	The next release of each version of Asterisk will contain, in addition to the fix for the “ExternalIVR” application, an updated README-SERIOUSLY.bestpractices.txt file.

Resolution	Asterisk now checks for the “ExternalIVR” application when processing the Originate action. Additionally, the README-SERIOUSLY.bestpractices.txt file has been updated. It is highly recommended that, if AMI is utilized with accounts that have the “originate” class authorization, Asterisk is run under a defined user that does not have root permissions. Accounts with the “originate” class authorization should be treated in a similar manner to those with the “system” class authorization.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	All versions
Asterisk Open Source	10.x	All versions
Certified Asterisk	1.8.11	All versions
Asterisk Digiumphones	10.x.x-digiumphones	All versions
Asterisk Business Edition	C.3.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.15.1, 10.7.1
Certified Asterisk	1.8.11-cert6
Asterisk Digiumphones	10.7.1-digiumphones
Asterisk Business Edition	C.3.7.6

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2012-012-1.8.diff	Asterisk 1.8
http:downloads.asterisk.org/pub/security/AST-2012-012-10.diff	Asterisk 10

Links	https://issues.asterisk.org/jira/browse/ASTERISK-20132

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-2012-012.pdf and http://downloads.digium.com/pub/security/AST-2012-012.html

Revision History		
Date	**Editor**	**Revisions Made**
08/27/2012	Matt Jordan	Initial version