Product	Asterisk
Summary	Asterisk Manager User Shell Access
Nature of Advisory	Permission Escalation
Susceptibility	Remote Authenticated Sessions
Severity	Minor
Exploits Known	Yes
Reported On	February 10, 2011
Reported By	Mark Murawski <markm AT intellasoft DOT net>
Posted On	April 21, 2011
Last Updated On	April 25, 2011
Advisory Contact	Matthew Nicholson <mnicholson@digium.com>
CVE Name	

Description	It is possible for a user of the Asterisk Manager Interface to bypass a security check and execute shell commands when they should not have that ability. Sending the “Async” header with the “Application” header during an Originate action, allows authenticated manager users to execute shell commands. Only users with the “system” privilege should be able to do this.

Resolution	Asterisk now performs the proper access check where appropriate during the originate manager action.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.6.1.x	All versions
Asterisk Open Source	1.6.2.x	All versions
Asterisk Open Source	1.8.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.6.1.25, 1.6.2.17.3, 1.8.3.3

Patches	
URL	**Branch**
http://downloads.asterisk.org/pub/security/AST-2011-006-1.6.1.diff	1.6.1
http://downloads.asterisk.org/pub/security/AST-2011-006-1.6.2.diff	1.6.2
http://downloads.asterisk.org/pub/security/AST-2011-006-1.8.diff	1.8

Links	

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2011-006.pdf and http://downloads.digium.com/pub/security/AST-2011-006.html

Revision History		
Date	**Editor**	**Revisions Made**
4/21/11	Matthew Nicholson	Initial version
4/25/11	Matthew Nicholson	Removed 1.4 and C.3 from this advisory due to a regression the fix causes.