Asterisk Project Security Advisory - AST-2017-006

Product	Asterisk
Summary	Shell access command injection in app_minivm
Nature of Advisory	Unauthorized command execution
Susceptibility	Remote Authenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	July 1, 2017
Reported By	Corey Farrell
Posted On	August 31, 2017
Last Updated On	August 31, 2017
Advisory Contact	Richard Mudgett <rmudgett AT digium DOT com>
CVE Name	CVE-2017-14100

Description	The app_minivm module has an “externnotify” program configuration option that is executed by the MinivmNotify dialplan application. The application uses the caller-id name and number as part of a built string passed to the OS shell for interpretation and execution. Since the caller-id name and number can come from an untrusted source, a crafted caller-id name or number allows an arbitrary shell command injection.

Resolution	Patched Asterisk’s app_minivm module to use a different system call that passes argument strings in an array instead of having the OS shell determine the application parameter boundaries.

Affected Versions

Product	**Release Series**	
Asterisk Open Source	11.x	All releases
Asterisk Open Source	13.x	All releases
Asterisk Open Source	14.x	All releases
Certified Asterisk	11.6	All releases
Certified Asterisk	13.13	All releases

Corrected In	
Product	**Release**
Asterisk Open Source	11.25.2, 13.17.1, 14.6.1
Certified Asterisk	11.6-cert17, 13.13-cert5

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2017-006-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2017-006-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2017-006-14.diff	Asterisk 14
http://downloads.asterisk.org/pub/security/AST-2017-006-11.6.diff	Certified Asterisk 11.6
http://downloads.asterisk.org/pub/security/AST-2017-006-13.13.diff	Certified Asterisk 13.13

Links	https://issues.asterisk.org/jira/browse/ASTERISK-27103

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2017-006.pdf and http://downloads.digium.com/pub/security/AST-2017-006.html

Revision History		
Date	**Editor**	**Revisions Made**
July 11, 2017	Richard Mudgett	Initial document created
August 31, 2017	Kevin Harwell	Updated for CVE