Product	Asterisk
Summary	Mitigation for libcURL HTTP request injection vulnerability
Nature of Advisory	HTTP request injection
Susceptibility	Remote Authenticated Sessions
Severity	Major
Exploits Known	No
Reported On	12 January, 2015
Reported By	Olle Johansson
Posted On	January 12, 2015
Last Updated On	January 28, 2015
Advisory Contact	Mark Michelson <mmichelson AT digium DOT com>
CVE Name	N/A.

Description	CVE-2014-8150 reported an HTTP request injection vulnerability in libcURL. Asterisk uses libcURL in its func_curl.so module (the CURL() dialplan function), as well as its res_config_curl.so (cURL realtime backend) modules. Since Asterisk may be configured to allow for user-supplied URLs to be passed to libcURL, it is possible that an attacker could use Asterisk as an attack vector to inject unauthorized HTTP requests if the version of libcURL installed on the Asterisk server is affected by CVE-2014-8150.

Resolution	Asterisk has been patched with a similar patch as libcURL was for CVE-2014-8150. This means that carriage return and linefeed characters are forbidden from being in HTTP URLs that will be passed to libcURL.

Affected Versions		
Product	**Release Series**	
Asteris Open Source	1.8.x	All versions
Asterisk Open Source	11.x	All versions
Asterisk Open Source	12.x	All versions
Asterisk Open Source	13.x	All versions
Certified Asterisk	1.8.28	All versions
Certified Asterisk	11.6	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.32.2, 11.15.1, 12.8.1, 13.1.1
Certified Asterisk	1.8.28-cert4, 11.6-cert10

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2015-002-1.8.28.diff	Certified Asterisk 1.8.28
http://downloads.asterisk.org/pub/security/AST-2015-002-11.6.diff	Certified Asterisk 11.6
http://downloads.asterisk.org/pub/security/AST-2015-002-1.8.diff	Asterisk 1.8
http://downloads.asterisk.org/pub/security/AST-2015-002-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2015-002-12.diff	Asterisk 12
http://downloads.asterisk.org/pub/security/AST-2015-002-13.diff	Asterisk 13

Links	https://issues.asterisk.org/jira/browse/ASTERISK-24676

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2015-002.pdf and http://downloads.digium.com/pub/security/AST-2015-002.html

Revision History		
Date	**Editor**	**Revisions Made**
21 January, 2015	Mark Michelson	Initial creation of document