Product	Asterisk
Summary	Stack Overflow in HTTP Processing of Cookie Headers.
Nature of Advisory	Denial Of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	February 21, 2014
Reported By	Lucas Molas, researcher at Programa STIC, Fundación Dr. Manuel Sadosky, Buenos Aires, Argentina
Posted On	March 10, 2014
Last Updated On	March 10, 2014
Advisory Contact	Richard Mudgett <rmudgett AT digium DOT com>
CVE Name	CVE-2014-2286

Description	Sending a HTTP request that is handled by Asterisk with a large number of Cookie headers could overflow the stack. You could even exhaust memory if you sent an unlimited number of headers in the request.

Resolution	The patched versions now handle headers in a fashion that prevents a stack overflow. Users should upgrade to a corrected version, apply the released patches, or disable HTTP support.

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

Corrected In

Product	Release
Asterisk Open Source	1.8.26.1, 11.8.1, 12.1.1
Certified Asterisk	1.8.15-cert5, 11.6-cert2

Patches

SVN URL	Revision
http://downloads.asterisk.org/pub/security/AST-2014-001-1.8.diff	Asterisk 1.8
http://downloads.asterisk.org/pub/security/AST-2014-001-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2014-001-12.diff	Asterisk 12
http://downloads.asterisk.org/pub/security/AST-2014-001-1.8.15.diff	Certified Asterisk 1.8.15
http://downloads.asterisk.org/pub/security/AST-2014-001-11.6.diff	Certified Asterisk 11.6

Links	https://issues.asterisk.org/jira/browse/ASTERISK-23340

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2014-001.pdf and http://downloads.digium.com/pub/security/AST-2014-001.html

Revision History

Date	Editor	Revisions Made
03/10/14	Richard Mudgett	Initial Revision.