Product	Asterisk
Summary	Denial of Service in HTTP server
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Major
Exploits Known	None
Reported On	January 21, 2013
Reported By	Christoph Hebeisen, TELUS Security Labs
Posted On	March 27, 2013
Last Updated On	March 27, 2013
Advisory Contact	Mark Michelson <mmichelson AT digium DOT com>
CVE Name	CVE-2013-2686

Description	AST-2012-014 [1], fixed in January of this year, contained a fix for Asterisk's HTTP server since it was susceptible to a remotely-triggered crash. The fix put in place fixed the possibility for the crash to be triggered, but a possible denial of service still exists if an attacker sends one or more HTTP POST requests with very large Content-Length values. [1] http://downloads.asterisk.org/pub/security/AST-2012-014.html

Resolution	Content-Length is now capped at a maximum value of 1024 bytes. Any attempt to send an HTTP POST with content-length greater than this cap will not result in any memory allocated. The POST will be responded to with an HTTP 413 “Request Entity Too Large” response.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	1.8.19.1, 1.8.20.0, 1.8.20.1
Asterisk Open Source	10.x	10.11.1, 10.12.0, 10.12.1
Asterisk Open Source	11.x	11.1.2, 11.2.0, 11.2.1
Certified Asterisk	1.8.15	1.8.15-cert1
Asterisk Digiumphones	10.x-digiumphones	10.11.1-digiumphones, 10.12.0-digiumphones, 10.12.1-digiumphones

Corrected In	
Product	**Release**
Asterisk Open Source	1.8.20.2, 10.12.2, 11.2.2
Certified Asterisk	1.8.15-cert2
Asterisk Digiumphones	10.12.2-digiumphones

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2013-002-1.8.diff	Asterisk 1.8
http://downloads.asterisk.org/pub/security/AST-2013-002-10.diff	Asterisk 10
http://downloads.asterisk.org/pub/security/AST-2013-002-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2013-002-1.8.15-cert.diff	Certified Asterisk 1.8.15

Links	https://issues.asterisk.org/jira/browse/ASTERISK-20967 http://telussecuritylabs.com/threats/show/TSL20130327-01

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2013-002.pdf and http://downloads.digium.com/pub/security/AST-2013-002.html

Revision History		
Date	**Editor**	**Revisions Made**

February 12, 2013	Mark Michelson	Initial Draft
March 27, 2013	Matt Jordan	Updated CVE
March 27, 2013	Matt Jordan	Updated with correct links to patches