Product	Asterisk
Summary	Remote Crash Vulnerability in WebSocket Server
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	30 October 2014
Reported By	Badalian Vyacheslav
Posted On	10 December 2014
Last Updated On	December 22, 2014
Advisory Contact	Joshua Colp <jcolp AT digium DOT com>
CVE Name	CVE-2014-9374

Description	When handling a WebSocket frame the res_http_websocket module dynamically changes the size of the memory used to allow the provided payload to fit. If a payload length of zero was received the code would incorrectly attempt to resize to zero. This operation would succeed and end up freeing the memory but be treated as a failure. When the session was subsequently torn down this memory would get freed yet again causing a crash. Users of the WebSocket functionality also did not take into account that provided text frames are not guaranteed to be NULL terminated. This has been fixed in chan_sip and chan_pjsip in the applicable versions.

Resolution	Ensure the built-in HTTP server is disabled, upgrade to a version listed below, or apply the applicable patch. The change ensures that res_http_websocket does not treat the freeing of memory when a payload length of zero is received as fatal.

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

Corrected In	
Product	**Release**
Certified Asterisk	11.6-cert9
Asterisk Open Source	11.14.2, 12.7.2, 13.0.2

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2014-019-11.6.diff	Certified Asterisk 11.6
http://downloads.asterisk.org/pub/security/AST-2014-019-11.diff	Asterisk 11
http://downloads.asterisk.org/pub/security/AST-2014-019-12.diff	Asterisk 12
http://downloads.asterisk.org/pub/security/AST-2014-019-13.diff	Asterisk 13

Links	https://issues.asterisk.org/jira/browse/ASTERISK-24472

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2014-019.pdf and http://downloads.digium.com/pub/security/AST-2014-019.html

Revision History		
Date	**Editor**	**Revisions Made**
December 10 2014	Joshua Colp	Initial Revision

December 22 2014	Matt Jordan	Added CVE