Product	Asterisk
Summary	Remote crash based on malformed SIP subscription requests
Nature of Advisory	Remotely triggered crash of Asterisk
Susceptibility	Remote authenticated sessions
Severity	Major
Exploits Known	No
Reported On	30 July, 2014
Reported By	Mark Michelson
Posted On	18 September, 2014
Last Updated On	September 18, 2014
Advisory Contact	Mark Michelson <mmichelson AT digium DOT com>
CVE Name	CVE-2014-6609

Description	It is possible to trigger a crash in Asterisk by sending a SIP SUBSCRIBE request with unexpected mixes of headers for a given event package. The crash occurs because Asterisk allocates data of one type at one layer and then interprets the data as a separate type at a different layer. The crash requires that the SUBSCRIBE be sent from a configured endpoint, and the SUBSCRIBE must pass any authentication that has been configured. Note that this crash is Asterisk's PJSIP-based res_pjsip_pubsub module and not in the old chan_sip module.

Resolution	Type-safety has been built into the pubsub API where it previously was absent. A test has been added to the testsuite that previously would have triggered the crash.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	1.8.x	Unaffected
Asterisk Open Source	11.x	Unaffected
Asterisk Open Source	12.x	12.1.0 and up
Certified Asterisk	1.8.15	Unaffected
Certified Asterisk	11.6	Unaffected

Corrected In	
Product	**Release**
Asterisk Open Source	12.5.1

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2014-009-12.diff	Asterisk 12

Links	https://issues.asterisk.org/jira/browse/ASTERISK-24136

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2014-009.pdf and http://downloads.digium.com/pub/security/AST-2014-009.html

Revision History		
Date	**Editor**	**Revisions Made**
19 August, 2014	Mark Michelson	Initial version of document
18 September, 2014	Matt Jordan	Added CVE