Product	Asterisk
Summary	Unauthenticated calls in chan_sip
Nature of Advisory	Authentication Bypass
Susceptibility	Remote unauthenticated sessions
Severity	Minor
Exploits Known	No
Reported On	October 3, 2016
Reported By	Walter Doekes
Posted On	December 8, 2016
Last Updated On	December 13, 2016
Advisory Contact	Mmichelson AT digium DOT com
CVE Name	CVE-2016-9938

Description	The chan_sip channel driver has a liberal definition for whitespace when attempting to strip the content between a SIP header name and a colon character. Rather than following RFC 3261 and stripping only spaces and horizontal tabs, Asterisk treats any non-printable ASCII character as if it were whitespace. This means that headers such as Contact\x01: will be seen as a valid Contact header. This mostly does not pose a problem until Asterisk is placed in tandem with an authenticating SIP proxy. In such a case, a crafty combination of valid and invalid To headers can cause a proxy to allow an INVITE request into Asterisk without authentication since it believes the request is an in-dialog request. However, because of the bug described above, the request will look like an out-of-dialog request to Asterisk. Asterisk will then process the request as a new call. The result is that Asterisk can process calls from unvetted sources without any authentication. If you do not use a proxy for authentication, then this issue does not affect you. If your proxy is dialog-aware (meaning that the proxy keeps track of what dialogs are currently valid), then this issue does not affect you. If you use chan_pjsip instead of chan_sip, then this issue does not affect you.

Resolution	chan_sip has been patched to only treat spaces and horizontal tabs as whitespace following a header name. This allows for Asterisk and authenticating proxies to view requests the same way

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	11.x	All Releases
Asterisk Open Source	13.x	All Releases
Asterisk Open Source	14.x	All Releases
Certified Asterisk	13.8	All Releases

Corrected In	
Product	**Release**
Asterisk Open Source	11.25.1, 13.13.1, 14.2.1
Certified Asterisk	11.6-cert16, 13.8-cert4

Patches	
SVN URL	**Revision**

Links	

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/ASTERISK-2016-009.pdf and http://downloads.digium.com/pub/security/ASTERISK-2016-009.html

Revision History		
Date	**Editor**	**Revisions Made**
November 28, 2016	Mark Michelson	Initial writeup
December 13, 2016	Kevin Harwell	Added description and CVE