Product	Asterisk
Summary	Crash when receiving SUBSCRIBE request
Nature of Advisory	Remote Crash
Susceptibility	Remote Unauthenticated Sessions
Severity	Major
Exploits Known	No
Reported On	January 30, 2018
Reported By	Sandro Gauci
Posted On	February 21, 2018
Last Updated On	February 21, 2018
Advisory Contact	Joshua Colp <jcolp AT digium DOT com>
CVE Name	CVE-2018-7284

Description	When processing a SUBSCRIBE request the res_pjsip_pubsub module stores the accepted formats present in the Accept headers of the request. This code did not limit the number of headers it processed despite having a fixed limit of 32. If more than 32 Accept headers were present the code would write outside of its memory and cause a crash.

Resolution	The res_pjsip_pubsub module has been changed to enforce a limit on the maximum number of Accept headers it will process. To receive this change upgrade to the version of Asterisk where this is resolved or apply the appropriate provided patch.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	13.x	All versions
Asterisk Open Source	14.x	All versions
Asterisk Open Source	15.x	All versions
Certified Asterisk	13.18	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	13.19.2, 14.7.6, 15.2.2
Certified Asterisk	13.18-cert3

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2018-004-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2018-004-14.diff	Asterisk 14
http://downloads.asterisk.org/pub/security/AST-2018-004-15.diff	Asterisk 15
http://downloads.asterisk.org/pub/security/AST-2018-004-13.18.diff	Certified Asterisk 13.18

Links	https://issues.asterisk.org/jira/browse/ASTERISK-27640

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2018-004.pdf and http://downloads.digium.com/pub/security/AST-2018-004.html

Revision History		
Date	**Editor**	**Revisions Made**
February 5, 2018	Joshua Colp	Initial Revision
February 21, 2018	Joshua Colp	Added CVE