Product	Asterisk
Summary	Buffer overflow in pjproject header parsing can cause crash in Asterisk
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	October 5, 2017
Reported By	Youngsung Kim at LINE Corporation
Posted On	
Last Updated On	October 25, 2017
Advisory Contact	gjoseph AT digium DOT com
CVE Name	

Description	By carefully crafting invalid values in the Cseq and the Via header port, pjproject's packet parsing code can create strings larger than the buffer allocated to hold them. This will usually cause Asterisk to crash immediately. The packets do not have to be authenticated.

Resolution	Stricter validation is now done on strings that represent numeric values before they are converted to intrinsic types. Invalid values now cause packet processing to stop and error messages to be emitted.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	13.x	All Releases
Asterisk Open Source	14.x	All Releases
Asterisk Open Source	15.x	All Releases
Certified Asterisk	13.13	All Releases

Copyright © 2017 Digium, Inc. All Rights Reserved.
Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.

Corrected In	
Product	**Release**
Asterisk Open Source	13.18.1, 14.7.1, 15.1.1
Certified Asterisk	13.13-cert7

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2017-009-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2017-009-14.diff	Asterisk 14
http://downloads.asterisk.org/pub/security/AST-2017-009-15.diff	Asterisk 15
http://downloads.asterisk.org/pub/security/AST-2017-009-13.13.diff	Certified Asterisk 13.13

Links	https://issues.asterisk.org/jira/browse/ASTERISK-27319

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2017-009.pdf and http://downloads.digium.com/pub/security/AST-2017-009.html

Revision History		
Date	**Editor**	**Revisions Made**
October 25, 2017	George Joseph	Initial Revision

Copyright © 2017 Digium, Inc. All Rights Reserved.
Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.