Product	Asterisk
Summary	Buffer Overrun in PJSIP transaction layer
Nature of Advisory	Buffer Overrun/Crash
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	12 April, 2017
Reported By	Sandro Gauci
Posted On	
Last Updated On	April 13, 2017
Advisory Contact	Mark Michelson <mark DOT michelson AT digium DOT com>
CVE Name	

Description	A remote crash can be triggered by sending a SIP packet to Asterisk with a specially crafted CSeq header and a Via header with no branch parameter. The issue is that the PJSIP RFC 2543 transaction key generation algorithm does not allocate a large enough buffer. By overrunning the buffer, the memory allocation table becomes corrupted, leading to an eventual crash. This issue is in PJSIP, and so the issue can be fixed without performing an upgrade of Asterisk at all. However, we are releasing a new version of Asterisk with the bundled PJProject updated to include the fix. If you are running Asterisk with chan_sip, this issue does not affect you.

Resolution	A patch created by the Asterisk team has been submitted and accepted by the PJProject maintainers.

Affected Versions

Product	Release Series	
Asterisk Open Source	11.x	Unaffected
Asterisk Open Source	13.x	All versions
Asterisk Open Source	14.x	All versions
Certified Asterisk	13.13	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	13.15.1, 14.4.1
Certified Asterisk	13.13-cert4

Patches	
SVN URL	**Revision**

Links	https://issues.asterisk.org/jira/browse/ASTERISK-26938

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2017-002.pdf and http://downloads.digium.com/pub/security/AST-2017-002.html

Revision History		
Date	**Editor**	**Revisions Made**
12 April, 2017	Mark Michelson	Initial report created