Product	Asterisk
Summary	Buffer overflow in CDR's set user
Nature of Advisory	Buffer Overflow
Susceptibility	Remote Authenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	October 9, 2017
Reported By	Richard Mudgett
Posted On	
Last Updated On	November 10, 2017
Advisory Contact	Rmudgett AT digium DOT com
CVE Name	CVE-2017-16671

Description	No size checking is done when setting the user field for Party B on a CDR. Thus, it is possible for someone to use an arbitrarily large string and write past the end of the user field storage buffer. The earlier AST-2017-001 advisory for the CDR user field overflow was for the Party A buffer. This currently affects any system using CDR's that also make use of the following: * The 'X-ClientCode' header within a SIP INFO message when using chan_sip and the 'useclientcode' option is enabled (note, it's disabled by default). * The CDR dialplan function executed from AMI when setting the user field. * The AMI Monitor action when using a long file name/path.

Resolution	The CDR engine now only copies up to the maximum allowed characters into the user field. Any characters outside the maximum are truncated.

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

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-2017-010-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2017-010-14.diff	Asterisk 14
http://downloads.asterisk.org/pub/security/AST-2017-010-15.diff	Asterisk 15
http://downloads.asterisk.org/pub/security/AST-2017-010-13.13.diff	Certified Asterisk 13.13

Links	https://issues.asterisk.org/jira/browse/ASTERISK-27337 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-16671

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2017-010.pdf and http://downloads.digium.com/pub/security/AST-2017-010.html

Revision History		
Date	**Editor**	**Revisions Made**
October 12, 2017	Richard Mudgett	Initial Revision