Product	Asterisk
Summary	Remote Crash Vulnerability in chan_sip channel driver
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	June 28, 2019
Reported By	Francesco Castellano
Posted On	July 1, 2019
Last Updated On	July 2, 2019
Advisory Contact	Jcolp AT sangoma DOT com
CVE Name	CVE-2019-13161

Description	When T.38 faxing is done in Asterisk a T.38 reinvite may be sent to an endpoint to switch it to T.38. If the endpoint responds with an improperly formatted SDP answer including both a T.38 UDPTL stream and an audio or video stream containing only codecs not allowed on the SIP peer or user a crash will occur. The code incorrectly assumes that there will be at least one common codec when T.38 is also in the SDP answer. This requires Asterisk to initiate a T.38 reinvite which is only done when executing the ReceiveFax dialplan application or performing T.38 passthrough where a remote endpoint has requested T.38. For versions of Asterisk 13 before 13.21.0 and Asterisk 15 before 15.4.0 the “preferred_codec_only” option must also be set to “yes”. If set to “no” the crash will not occur.

Resolution	If T.38 faxing is not required this functionality can be disabled by ensuring the “t38pt_udptl” is set to “no” so a T.38 reinvite is not possible. If T.38 faxing is required then Asterisk should be upgraded to a fixed version. The problem can also be limited in scope by enabling T.38 faxing only for endpoints which actually participate in fax.

Copyright © 2019 Digium, Inc. All Rights Reserved.
Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	13.x	All releases
Asterisk Open Source	15.x	All releases
Asterisk Open Source	16.x	All releases
Certified Asterisk	13.21	All releases

Corrected In	
Product	**Release**
Asterisk Open Source	13.27.1
Asterisk Open Source	15.7.3
Asterisk Open Source	16.4.1
Certified Asterisk	13.21-cert4

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2019-003-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2019-003-15.diff	Asterisk 15
http://downloads.asterisk.org/pub/security/AST-2019-003-16.diff	Asterisk 16
http://downloads.asterisk.org/pub/security/AST-2019-003-13.21.diff	Certified Asterisk 13.21

Links	https://issues.asterisk.org/jira/browse/ASTERISK-28465

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-2019-003.pdf and http://downloads.digium.com/pub/security/AST-2019-003.html

Revision History

Copyright © 2019 Digium, Inc. All Rights Reserved.
Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.

Date	Editor	Revisions Made
July 1, 2019	Joshua Colp	Initial revision

Copyright © 2019 Digium, Inc. All Rights Reserved.
Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.