Product	Asterisk
Summary	Remote Crash Vulnerability in PJSIP channel driver
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	December 4, 2020
Reported By	Mauri de Souza Meneguzzo (3CPlus)
Posted On	February 8, 2021
Last Updated On	February 8, 2021
Advisory Contact	Jcolp AT sangoma DOT com
CVE Name	CVE-2021-26906

Description	Given a scenario where an outgoing call is placed from Asterisk to a remote SIP server it is possible for a crash to occur. The code responsible for negotiating SDP in SIP responses incorrectly assumes that SDP negotiation will always be successful. If a SIP response containing an SDP that can not be negotiated is received a subsequent SDP negotiation on the same call can cause a crash. If the “accept_multiple_sdp_answers” option in the “system” section of pjsip.conf is set to “yes” then any subsequent non-forked SIP response with SDP can trigger this crash. If the “follow_early_media_fork” option in the “system” section of pjsip.conf is set to “yes” (the default) then any subsequent SIP responses with SDP from a forked destination can trigger this crash. If a 200 OK with SDP is received from a forked destination it can also trigger this crash, even if the “follow_early_media_fork” option is not set to “yes”. In all cases this relies on a race condition with tight timing where the second SDP negotiation occurs before termination of the call due to the initial SDP negotiation failure.
Modules Affected	res_pjsip_session.c, PJSIP

Resolution	The issue has been fixed in PJSIP by changing the behavior of the

	pjmedia_sdp_neg_modify_local_offer2 function. If SDP was previously negotiated the code no longer assumes that it was successful and instead checks that SDP was negotiated. This issue can only be resolved by upgrading to a fixed version or applying the provided patch.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	13.x	All versions
Asterisk Open Source	16.x	All versions
Asterisk Open Source	17.x	All versions
Asterisk Open Source	18.x	All versions
Certified Asterisk	16.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	13.38.2, 16.16.1, 17.9.2, 18.2.1
Certified Asterisk	16.8-cert6

Patches	
Patch URL	**Revision**
https://downloads.asterisk.org/pub/security/AST-2021-005-13.diff	Asterisk 13
https://downloads.asterisk.org/pub/security/AST-2021-005-16.diff	Asterisk 16
https://downloads.asterisk.org/pub/security/AST-2021-005-17.diff	Asterisk 17
https://downloads.asterisk.org/pub/security/AST-2021-005-18.diff	Asterisk 18
https://downloads.asterisk.org/pub/security/AST-2021-005-16.8.diff	Certified Asterisk 16.8

Links	https://issues.asterisk.org/jira/browse/ASTERISK-29196 https://downloads.asterisk.org/pub/security/AST-2021-005.html

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-2021-005.pdf and http://downloads.digium.com/pub/security/AST-2021-005.html

Revision History		
Date	**Editor**	**Revisions Made**
February 8, 2021	Joshua Colp	Initial revision