Product	Asterisk
Summary	Remote crash possible when negotiating T.38
Nature of Advisory	Denial of service
Susceptibility	Remote authenticated sessions
Severity	Minor
Exploits Known	No
Reported On	December 8, 2020
Reported By	Gregory Massel
Posted On	
Last Updated On	February 4, 2021
Advisory Contact	kharwell AT sangoma DOT com
CVE Name	

Description	When re-negotiating for T.38 if the initial remote response was delayed just enough Asterisk would send both audio and T.38 in the SDP. If this happened, and the remote responded with a declined T.38 stream then Asterisk would crash.
Modules Affected	res_pjsip_session.c, res_pjsip_t38.c

Resolution	When re-negotiating for T.38, and a delay occurs Asterisk now sends SDP only for the expected T.38 stream. A check was also put in place to ensure an active T.38 media stream is active within Asterisk when attempting to change state for fax.

Affected Versions		
Product	**Release Series**	**Introduced**
Asterisk Open Source	16.x	16.15.0
Asterisk Open Source	17.x	17.9.0
Asterisk Open Source	18.x	18.1.0
Certified Asterisk	16.8	16.8-cert4

Corrected In	
Product	**Release**
Asterisk Open Source	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-2021-002-16.diff	Asterisk 16
https://downloads.asterisk.org/pub/security/AST-2021-002-17.diff	Asterisk 17
https://downloads.asterisk.org/pub/security/AST-2021-002-18.diff	Asterisk 18
https://downloads.asterisk.org/pub/security/AST-2021-002-16.8.diff	Certified Asterisk 16.8-cert6

Links	https://issues.asterisk.org/jira/browse/ASTERISK-29203 https://downloads.asterisk.org/pub/security/AST-2021-002.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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2021-002.pdf and http://downloads.digium.com/pub/security/AST-2021-002.html

Revision History		
Date	**Editor**	**Revisions Made**
February 1, 2021	Kevin Harwell	Initial revision