Product	Asterisk
Summary	Remote crash in res_pjsip_session
Nature of Advisory	Denial of service
Susceptibility	Remote authenticated sessions
Severity	Moderate
Exploits Known	No
Reported On	August 31, 2020
Reported By	Sandro Gauci
Posted On	
Last Updated On	October 27, 2020
Advisory Contact	kharwell AT sangoma DOT com
CVE Name	

Description	Upon receiving a new SIP Invite, Asterisk did not return the created dialog locked or referenced. This caused a “gap” between the creation of the dialog object, and its next use by the thread that created it. Depending upon some off nominal circumstances, and timing it was possible for another thread to free said dialog in this “gap”. Asterisk could then crash when the dialog object, or any of its dependent objects were de-referenced, or accessed next by the initial creation thread. Note, however that this crash can only occur when using a connection oriented protocol (e.g. TCP, TLS) for the SIP transport. If you are using UDP then your system should not be affected. As well, the remote client must be authenticated, or Asterisk must be configured for anonymous calling in order for this problem to manifest.
Modules Affected	res_pjsip.c, res_pjsip_session.c, res_pjsip_pubsub.c

Resolution	Asterisk now returns the newly created dialog object both locked, and with its reference count increased. The lock, and added reference are then held until such a time it is safe to release both the lock, and decrement the reference count.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	13.x	All releases
Asterisk Open Source	16.x	All releases
Asterisk Open Source	17.x	All releases
Asterisk Open Source	18.x	All releases
Certified Asterisk	16.8	All releases

Corrected In	
Product	**Release**
Asterisk Open Source	13.37.1, 16.15.1, 17.8.1, 18.1.1
Certified Asterisk	16.8-cert4

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2020-001-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2020-001-16.diff	Asterisk 16
http://downloads.asterisk.org/pub/security/AST-2020-001-17.diff	Asterisk 17
http://downloads.asterisk.org/pub/security/AST-2020-001-18.diff	Asterisk 18
http://downloads.asterisk.org/pub/security/AST-2020-001-16.8.diff	Certified Asterisk 16.8-cert4

Links	https://issues.asterisk.org/jira/browse/ASTERISK-29057

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2020-001.pdf and http://downloads.digium.com/pub/security/AST-2020-001.html

Revision History		
Date	**Editor**	**Revisions Made**
October 19, 2020	Kevin Harwell	Initial revision