Asterisk Project Security Advisory – AST-2020-002

Product	Asterisk
Summary	Outbound INVITE loop on challenge with different nonce.
Nature of Advisory	Denial of Service
Susceptibility	Remote Authenticated Sessions
Severity	Minor
Exploits Known	Yes
Reported On	July 28, 2020
Reported By	Sebastian Damm, Ruslan Lazin
Posted On	November 5, 2020
Last Updated On	November 5, 2020
Advisory Contact	bford AT sangoma DOT com
CVE Name	

Description	If Asterisk is challenged on an outbound INVITE and the nonce is changed in each response, Asterisk will continually send INVITEs in a loop. This causes Asterisk to consume more and more memory since the transaction will never terminate (even if the call is hung up), ultimately leading to a restart or shutdown of Asterisk. Outbound authentication must be configured on the endpoint for this to occur.
Modules Affected	res_pjsip

Resolution	In the fixed versions of Asterisk, a counter has been added that will automatically stop sending INVITEs after reaching the limit.

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	16.8	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	13.37.1
Asterisk Open Source	16.14.1
Asterisk Open Source	17.8.1
Asterisk Open Source	18.0.1
Certified Asterisk	16.8-cert5

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2020-002-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2020-002-16.diff	Asterisk 16
http://downloads.asterisk.org/pub/security/AST-2020-002-17.dif	Asterisk 17
http://downloads.asterisk.org/pub/security/AST-2020-002-18.dif	Asterisk 18
http://downloads.asterisk.org/pub/security/AST-2020-002-16.8.diff	Certified Asterisk 16.8-cert5

Links	https://issues.asterisk.org/jira/browse/ASTERISK-29013

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2020-002.pdf and http://downloads.digium.com/pub/security/AST-2020-002.html

Revision History		
Date	**Editor**	**Revisions Made**
November 5, 2020	Ben Ford	Initial Revision