Product	Asterisk
Summary	SIP request can change address of a SIP peer.
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	October 17, 2019
Reported By	Andrey V. T.
Posted On	November 21, 2019
Last Updated On	November 21, 2019
Advisory Contact	bford AT sangoma DOT com
CVE Name	CVE-2019-18790

Description	A SIP request can be sent to Asterisk that can change a SIP peer's IP address. A REGISTER does not need to occur, and calls can be hijacked as a result. The only thing that needs to be known is the peer's name; authentication details such as passwords do not need to be known. This vulnerability is only exploitable when the "nat" option is set to the default, or "auto_force_rport".
Modules Affected	channels/chan_sip.c

Resolution	Using any other option value for "nat" will prevent the attack (such as "nat=no" or "nat=force_rport"), but will need to be tested on an individual basis to ensure that it works for the user's deployment. On the fixed versions of Asterisk, it will no longer set the address of the peer before authentication is successful when a SIP request comes in.

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
Certified Asterisk	13.21	All releases

Corrected In	
Product	**Release**
Asterisk Open Source	13.29.2
Asterisk Open Source	16.6.2
Asterisk Open Source	17.0.1
Certified Asterisk	13.21-cert5

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2019-006-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2019-006-16.diff	Asterisk 16
http://downloads.asterisk.org/pub/security/AST-2019-006-17.diff	Asterisk 17
http://downloads.asterisk.org/pub/security/AST-2019-006-13.21.diff	Certified Asterisk 13.21-cert5

Links	https://issues.asterisk.org/jira/browse/ASTERISK-28589

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2019-006.pdf and http://downloads.digium.com/pub/security/AST-2019-006.html

Revision History		
Date	**Editor**	**Revisions Made**
October 22, 2019	Ben Ford	Initial Revision
November 14, 2019	Ben Ford	Corrected and updated fields for versioning, and added CVE
November 21, 2019	Ben Ford	Added “Posted On” date