Product	Asterisk
Summary	Remote crash vulnerability with SDP protocol violation
Nature of Advisory	Denial Of Service
Susceptibility	Remote Authenticated Sessions
Severity	Low
Exploits Known	No
Reported On	January 24, 2019
Reported By	Sotiris Ganouris
Posted On	November 14,2018
Last Updated On	
Advisory Contact	gjoseph AT digium DOT com
CVE Name	CVE-2019-7251

Description	When Asterisk makes an outgoing call, a very specific SDP protocol violation by the remote party can cause Asterisk to crash.

Resolution	Upgrade Asterisk to a fixed version.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	15.x	All releases
Asterisk Open Source	16.x	All releases

Corrected In	
Product	**Release**
Asterisk Open Source	15.7.2
Asterisk Open Source	16.2.1

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/se	Asterisk 15

curity/AST-2019-001-15.diff	
http://downloads.asterisk.org/pub/se curity/AST-2019-001-16.diff	Asterisk 16

Links	https://issues.asterisk.org/jira/browse/ASTERISK-28260

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2019-001.pdf and http://downloads.digium.com/pub/security/AST-2019-001.html

Revision History		
Date	**Editor**	**Revisions Made**
January 31, 2019	George Joseph	Initial revision
March 1, 2019	Kevin Harwell	Updated diff hyperlinks