Product	Asterisk
Summary	Remote crash vulnerability with MESSAGE messages
Nature of Advisory	Denial Of Service
Susceptibility	Remote Authenticated Sessions
Severity	Low
Exploits Known	No
Reported On	June 13, 2019
Reported By	Gil Richard
Posted On	June 14,2019
Last Updated On	George Joseph
Advisory Contact	gjoseph AT digium DOT com
CVE Name	CVE-2019-12827

Description	A specially crafted SIP in-dialog MESSAGE message can cause Asterisk to crash.

Resolution	Upgrade Asterisk to a fixed version.

Affected Versions		
Product	**Release Series**	
Certified Asterisk	13.21-cert	All releases
Asterisk Open Source	13.x	All releases
Asterisk Open Source	15.x	All releases
Asterisk Open Source	16.x	All releases

Corrected In

Product	Release
Certified Asterisk	13.21-cert4
Asterisk Open Source	13.27.1
Asterisk Open Source	15.7.3
Asterisk Open Source	16.4.1

Patches

SVN URL	Revision
http://downloads.asterisk.org/pub/security/AST-2019-002-13.21.diff	Certified Asterisk 13.21-cert4
http://downloads.asterisk.org/pub/security/AST-2019-002-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2019-002-15.diff	Asterisk 15
http://downloads.asterisk.org/pub/security/AST-2019-002-16.diff	Asterisk 16

Links	https://issues.asterisk.org/jira/browse/ASTERISK-28447

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2019-002.pdf and http://downloads.digium.com/pub/security/AST-2019-002.html

Revision History

Date	Editor	Revisions Made
June 14, 2019	George Joseph	Initial revision