Product	Asterisk
Summary	Remote Crash Vulnerability in H323 channel add on
Nature of Advisory	Exploitable Stack Buffer Underflow
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	Yes
Reported On	
Reported By	
Posted On	
Last Updated On	November 30, 2022
Advisory Contact	mbradeen AT sangoma DOT com
CVE Name	CVE-2022-37325

Description	A zero length Called or Calling Party Number can cause a buffer under-run and Asterisk crash.
Modules Affected	ooh323

Resolution	If currently not loading the ooh323 module, no action is required. For others, please make sure that the h323 listen port is not publicly open and apply the patch when possible.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	16.x	All Versions
Asterisk Open Source	18.x	All Versions
Asterisk Open Source	19.x	All Versions
Asterisk Open Source	20.x	All Versions
Certified Asterisk	18.9.x	All Versions

Corrected In	
Product	**Release**
Asterisk Open Source	16.29.1, 18.15.1, 19.7.1, 20.0.1
Certified Asterisk	Certified-18.9-cert3

Patches	
Patch URL	**Revision**
https://downloads.digium.com/pub/security/AST-2022-007-16-16.diff	Asterisk 16
https://downloads.digium.com/pub/security/AST-2022-007-16-18.diff	Asterisk 18
https://downloads.digium.com/pub/security/AST-2022-007-16-17.diff	Asterisk 19
https://downloads.digium.com/pub/security/AST-2022-007-16-18.diff	Asterisk 20
https://downloads.digium.com/pub/security/AST-2022-007-16-18.9.diff	Certified Asterisk 18.9

Links	https://issues.asterisk.org/jira/browse/ASTERISK-30103 https://downloads.asterisk.org/pub/security/AST-2022-007.html

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This document may be superseded by later versions; if so, the latest version will be posted at https://downloads.digium.com/pub/security/AST-2022-007.pdf and https://downloads.digium.com/pub/security/AST-2022-007.html

Revision History		
Date	**Editor**	**Revisions Made**