Product	Asterisk
Summary	Remote crash when using IAX2 channel driver
Nature of Advisory	Denial of service
Susceptibility	Remote unauthenticated sessions
Severity	Major
Exploits Known	No
Reported On	April 13, 2021
Reported By	Michael Welk
Posted On	
Last Updated On	July 6, 2021
Advisory Contact	kharwell AT sangoma DOT com
CVE Name	CVE-2021-32558

Description	If the IAX2 channel driver receives a packet that contains an unsupported media format it can cause a crash to occur in Asterisk.
Modules Affected	chan_iax2.c

Resolution	Checks are now in place that make it so packets containing unsupported media formats are ignored/dropped in the IAX2 channel driver. This ensures Asterisk no longer crashes.

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	13.38.3, 16.19.1, 17.9.4, 18.5.1
Certified Asterisk	16.8-cert10

Patches	
Patch URL	**Revision**
http://downloads.digium.com/pub/security/AST-2021-008-13.diff	Asterisk 13
http://downloads.digium.com/pub/security/AST-2021-008-16.diff	Asterisk 16
http://downloads.digium.com/pub/security/AST-2021-008-17.diff	Asterisk 17
http://downloads.digium.com/pub/security/AST-2021-008-18.diff	Asterisk 18
http://downloads.digium.com/pub/security/AST-2021-008-16.8.diff	Certified Asterisk 16.8

Links	https://issues.asterisk.org/jira/browse/ASTERISK-29392 https://downloads.asterisk.org/pub/security/AST-2021-008.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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2021-008.pdf and
http://downloads.digium.com/pub/security/AST-2021-008.html

Revision History		
Date	**Editor**	**Revisions Made**
May 10, 2021	Kevin Harwell	Initial revision