Product	Asterisk
Summary	Remote Crash Vulnerability in audio transcoding
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	August 7, 2019
Reported By	Gregory Massel
Posted On	
Last Updated On	August 26, 2019
Advisory Contact	Jcolp AT sangoma DOT com
CVE Name	CVE-2019-15639

Description	When audio frames are given to the audio transcoding support in Asterisk the number of samples are examined and as part of this a message is output to indicate that no samples are present. A change was done to suppress this message for a particular scenario in which the message was not relevant. This change assumed that information about the origin of a frame will always exist when in reality it may not. This issue presented itself when an RTP packet containing no audio (and thus no samples) was received. In a particular transcoding scenario this audio frame would get turned into a frame with no origin information. If this new frame was then given to the audio transcoding support a crash would occur as no samples and no origin information would be present. The transcoding scenario requires the “genericplc” option to be set to enabled (the default) and a transcoding path from the source format into signed linear and then from signed linear into another format. Note that there may be other scenarios that have not been found which can cause an audio frame with no origin to be given to the audio transcoding support and thus cause a crash.
Modules Affected	main/translate.c

Resolution	The “genericplc” option can be disabled in codecs.conf to mitigate the described scenario. It is recommended, however, that Asterisk be upgraded to one of the listed versions or the linked patch applied to protect against potential unknown scenarios.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	13.x	13.28.0
Asterisk Open Source	16.x	16.5.0

Corrected In	
Product	**Release**
Asterisk Open Source	13.28.1
Asterisk Open Source	16.5.1

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2019-005-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2019-005-16.diff	Asterisk 16

Links	https://issues.asterisk.org/jira/browse/ASTERISK-28499

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2019-005.pdf and http://downloads.digium.com/pub/security/AST-2019-005.html

Revision History		
Date	**Editor**	**Revisions Made**
August 26, 2019	Joshua Colp	Initial revision