Product	Asterisk
Summary	Crash when receiving unnegotiated dynamic payload
Nature of Advisory	Remote Crash
Susceptibility	Remote Unauthenticated Sessions
Severity	Major
Exploits Known	No
Reported On	December 18, 2017
Reported By	Sébastien Duthil
Posted On	February 21, 2018
Last Updated On	February 21, 2018
Advisory Contact	Joshua Colp <jcolp AT digium DOT com>
CVE Name	CVE-2018-7285

Description	The RTP support in Asterisk maintains its own registry of dynamic codecs and desired payload numbers. While an SDP negotiation may result in a codec using a different payload number these desired ones are still stored internally. When an RTP packet was received this registry would be consulted if the payload number was not found in the negotiated SDP. This registry was incorrectly consulted for all packets, even those which are dynamic. If the payload number resulted in a codec of a different type than the RTP stream (for example the payload number resulted in a video codec but the stream carried audio) a crash could occur if no stream of that type had been negotiated. This was due to the code incorrectly assuming that a stream of the type would always exist.

Resolution	The RTP support will now only consult the registry for payloads which are statically defined. The core has also been changed to protect against situations where a frame of media is received for a media type that has not been negotiated. To receive these fixes update to the given version of Asterisk or apply the provided patch. There is no configuration which can protect against this vulnerability.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	13.x	Unaffected
Asterisk Open Source	14.x	Unaffected
Asterisk Open Source	15.x	All versions
Certified Asterisk	13.18	Unaffected

Corrected In	
Product	**Release**
Asterisk Open Source	15.2.2

Patches	
SVN URL	**Revision**
http://downloads.asterisk.org/pub/security/AST-2018-001-15.diff	Asterisk 15

Links	https://issues.asterisk.org/jira/browse/ASTERISK-27488

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2018-001.pdf and http://downloads.digium.com/pub/security/AST-2018-001.html

Revision History		
Date	**Editor**	**Revisions Made**
January 15, 2018	Joshua Colp	Initial Revision
February 21, 2018	Joshua Colp	Added CVE