Product	Asterisk
Summary	WebSocket frames with 0 sized payload causes DoS
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	February 05, 2018
Reported By	Sean Bright
Posted On	February 21, 2018
Last Updated On	February 21, 2018
Advisory Contact	bford AT digium DOT com
CVE Name	CVE-2018-7287

Description	When reading a websocket, the length was not being checked. If a payload of length 0 was read, it would result in a busy loop that waited for the underlying connection to close.

Resolution	A patch to asterisk is available that checks for payloads of size 0 before attempting to read them. By default, Asterisk does not enable the HTTP server, which means it is not vulnerable to this problem. If the HTTP server is enabled, you can disable it if you do not need it. Otherwise, the patch provided with this security vulnerability can be applied. Either of these approaches will resolve the problem.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	15.x	All versions

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

Patches

SVN URL	Revision
http://downloads.asterisk.org/pub/security/ AST-2018-006-15.diff	Asterisk 15

Links	https://issues.asterisk.org/jira/browse/ASTERISK-27658 http://downloads.asterisk.org/pub/security/AST-2018-006.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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2018-006.pdf and http://downloads.digium.com/pub/security/AST-2018-006.html

Revision History		
Date	**Editor**	**Revisions Made**
February 15, 2018	Ben Ford	Initial Revision
February 21, 2018	Ben Ford	Added CVE Name