

Asterisk Project Security Advisory - AST-2018-007

Product	Asterisk
Summary	Infinite loop when reading iostreams
Nature of Advisory	Denial of Service
Susceptibility	Remote Authenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	April 16, 2018
Reported By	Sean Bright
Posted On	
Last Updated On	April 25, 2018
Advisory Contact	Kevin Harwell <kharwell AT digium DOT com>
CVE Name	

Description	When connected to Asterisk via TCP/TLS if the client abruptly disconnects, or sends a specially crafted message then Asterisk gets caught in an infinite loop while trying to read the data stream. Thus rendering the system as unusable.
--------------------	--

Resolution	Stricter error checking is now done when iostreams encounters a problem. When an error occurs during reading it is now properly handled, and continued reading is appropriately stopped.
-------------------	--

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

Corrected In	
Product	Release
Asterisk Open Source	15.4.1

Asterisk Project Security Advisory - AST-2018-007

Copyright © 2018 Digium, Inc. All Rights Reserved.

Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.

Asterisk Project Security Advisory - AST-2018-007

Patches	
SVN URL	Revision
http://downloads.asterisk.org/pub/security/AST-2018-007-15.diff	Asterisk 15

Links	https://issues.asterisk.org/jira/browse/ASTERISK-27807
--------------	---

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This document may be superseded by later versions; if so, the latest version will be posted at 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-2018-007.pdf> and <http://downloads.digium.com/pub/security/AST-2018-007.html>

Revision History		
Date	Editor	Revisions Made
April 25, 2018	Kevin Harwell	Initial Revision

Asterisk Project Security Advisory - AST-2018-007

Copyright © 2018 Digium, Inc. All Rights Reserved.

Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.