Asterisk Project Security Advisory - AST-2017-004

Product	Asterisk
Summary	Memory exhaustion on short SCCP packets
Nature of Advisory	Denial of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Critical
Exploits Known	No
Reported On	April 13, 2017
Reported By	Sandro Gauci
Posted On	
Last Updated On	April 13, 2017
Advisory Contact	George Joseph <gjoseph AT digium DOT com>
CVE Name	

Description	A remote memory exhaustion can be triggered by sending an SCCP packet to Asterisk system with “chan_skinny” enabled that is larger than the length of the SCCP header but smaller than the packet length specified in the header. The loop that reads the rest of the packet doesn’t detect that the call to read() returned end-of-file before the expected number of bytes and continues infinitely. The “partial data” message logging in that tight loop causes Asterisk to exhaust all available memory.

Resolution	If support for the SCCP protocol is not required, remove or disable the module. If support for SCCP is required, an upgrade to Asterisk will be necessary.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	11.x	Unaffected
Asterisk Open Source	13.x	All versions
Asterisk Open Source	14.x	All versions
Certified Asterisk	13.13	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	13.15.1, 14.4.1
Certified Asterisk	13.13-cert4

Patches	
SVN URL	**Revision**

Links	

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/.pdf and http://downloads.digium.com/pub/security/.html

Revision History		
Date	**Editor**	**Revisions Made**
13 April 2017	George Joseph	Initial report created