

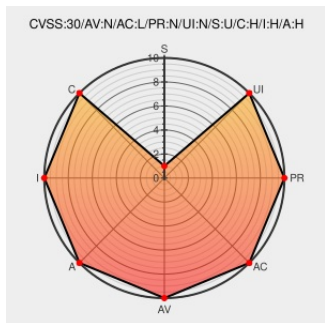


CVE-2015-2311

Published on: 08/09/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:20 PM UTC

CVE-2015-2311

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Capnproto](#) from [Capnproto](#) contain the following vulnerability:

Integer underflow in Sandstorm Cap'n Proto before 0.4.1.1 and 0.5.x before 0.5.1.1 might allow remote peers to cause a denial of service or possibly obtain sensitive information from memory or execute arbitrary code via a crafted message.

CVE-2015-2311 has been assigned by [@security@debian.org](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SECURITY: Integer underflow in pointer validation. · capnproto/capnproto@26bcced · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/capnproto/capnproto/commit/26bcceda72372211063d62aab7e45665faa8

oss-security - Re: CVE Request: Cap'n Proto: Several issues

Mailing List

Third Party Advisory

www.openwall.com

text/html

MLIST [oss-security] 20150317 Re: CVE Request: Cap'n Proto: Several issues

capnproto/2015-03-02-1-c++-integer-underflow.md at master · capnproto/capnproto · GitHub

Third Party Advisory

github.com

text/html

CONFIRM github.com/capnproto/capnproto/blob/master/security-advisories/2015-03-02-1-c%2B%2B-integer-underflow.md

#780566 - capnproto: CVE-2015-2311: Integer underflow in pointer validation - Debian Bug report logs

Mailing List

Third Party Advisory

bugs.debian.org

text/html

MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=780566

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Capnproto	Capnproto	0.5.0.0	All	All	All
Application	Capnproto	Capnproto	0.5.1.0	All	All	All
Application	Capnproto	Capnproto	All	All	All	All
Application	Capnproto	Capnproto	0.5.0.0	All	All	All
Application	Capnproto	Capnproto	0.5.1.0	All	All	All
cpe:2.3:a:capnproto:capnproto:0.5.0.0:*:*:*:*:*:						
cpe:2.3:a:capnproto:capnproto:0.5.1.0:*:*:*:*:*:						
cpe:2.3:a:capnproto:capnproto:*:*:*:*:*:						
cpe:2.3:a:capnproto:capnproto:0.5.0.0:*:*:*:*:*:						
cpe:2.3:a:capnproto:capnproto:0.5.1.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)