



CVE-2015-2688

Published on: 01/24/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:19 PM UTC

CVE-2015-2688

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

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

buf_pullup in Tor before 0.2.4.26 and 0.2.5.x before 0.2.5.11 does not properly handle unexpected arrival times of buffers with invalid layouts, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via crafted packets.

CVE-2015-2688 has been assigned by security@debian.org to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **The Tor Project** - **Tor** version **before 0.2.4.26**

Affected Vendor/Software: **The Tor Project** - **Tor** version **0.2.5.x before 0.2.5.11**

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
5 - HIGH	5 - HIGH	MITRE

[tor-talk] Pre-announcement: source for 1 or 0.2.4.26 and 0.2.5.11 is available.

Mailing List

Vendor Advisory

lists.torproject.org

text/html

✉

MISC

lists.torproject.org/pipermail/tor-talk/2015-March/037281.html

#15083 (Assertion ch->data < &ch->mem[0]+ch->memlen failed) – Tor Bug Tracker & Wiki

Patch

Vendor Advisory

trac.torproject.org

text/html

🔥

MISC

trac.torproject.org/projects/tor/ticket/15083

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	Torproject	Tor	All	All	All	All
Application	Torproject	Tor	All	All	All	All

cpe:2.3:a:torproject:tor:*****:

cpe:2.3:a:torproject:tor:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →