



CVE-2018-0491

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-0491
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-05 15:29:00 UTC
Updated	2019-03-26 18:52:00 UTC
Description	A use-after-free issue was discovered in Tor 0.3.2.x before 0.3.2.10. It allows remote attackers to cause a denial of service

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Torproject	Tor	All	All	All	All
Application	Torproject	Tor	All	All	All	All

References

Reference	Source	Li
New stable Tor releases, with security fixes and DoS prevention: 0.3.2.10, 0.3.1.10, 0.2.9.15 Tor Blog	CONFIRM	bl
#24700 (sched: With KIST, a channel can be added more than once in the pending list) – Tor Bug Tracker & Wiki	CONFIRM	tra
#25117 (Resolve TROVE-2018-002: bug 24700 KIST use-after-free can be remotely triggered) – Tor Bug Tracker & Wiki	CONFIRM	tra
Tor Browser < 0.3.2.10 - Use After Free (PoC) - Linux dos Exploit	EXPLOIT-DB	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[501257](#) Alpine Linux Security Update for tor

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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