



CVE-2021-38385

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

Summary

CVE	CVE-2021-38385
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-30 05:15:00 UTC
Updated	2023-05-03 12:15:00 UTC
Description	Tor before 0.3.5.16, 0.4.5.10, and 0.4.6.7 mishandles the relationship between batch-signature verification and single-signa

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Potential consensus divergence from Ed25519 edge cases (#40078) · Issues · The Tor Project / Core / Tor · GitLab	CONFIRM	bugs.torpro
Tor Blog The Tor Project	MISC	blog.torpro
New Stable Releases: Tor 0.3.5.16, 0.4.5.10 and 0.4.6.7 Tor Blog	CONFIRM	blog.torpro
Tor: Multiple Vulnerabilities (GLSA 202305-11) — Gentoo security	GENTOO	security.ge
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178771](#) Debian Security Update for tor (DSA 4961-1)

[184304](#) Debian Security Update for tor (CVE-2021-38385)

[001600](#) F... .. (FFDORA 0001 017 0710)

281839 Fedora Security Update for tor (FEDORA-2021-84/ca2/49a)
281847 Fedora Security Update for tor (FEDORA-2021-52d6a75d28)
501929 Alpine Linux Security Update for tor
502192 Alpine Linux Security Update for tor
710727 Gentoo Linux Tor Multiple Vulnerabilities (GLSA 202305-11)
751024 OpenSUSE Security Update for tor (openSUSE-SU-2021:1169-1)

© [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](#)