



CVE-2021-34549

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

Summary

CVE	CVE-2021-34549
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-29 12:15:00 UTC
Updated	2022-07-12 17:42:00 UTC
Description	An issue was discovered in Tor before 0.4.6.5, aka TROVE-2021-005. Hashing is mishandled for certain retrieval of circuit c

Risk And Classification

Problem Types: CWE-400

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	Tags
Not Found	MISC	gitlab.torproject.org	
Tor: Multiple vulnerabilities (GLSA 202107-25) — Gentoo security	GENTOO	security.gentoo.org	
New stable security releases: 0.3.5.15, 0.4.4.9, 0.4.5.9, 0.4.6.5 Tor Blog	CONFIRM	blog.torproject.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

178676 Debian Security Update for tor (DSA 4932-1)
180452 Debian Security Update for tor (CVE-2021-34549)
281659 Fedora Security Update for tor (FEDORA-2021-ff4ad9825a)
281660 Fedora Security Update for tor (FEDORA-2021-1b60c984e5)

501260 Alpine Linux Security Update for tor
710051 Gentoo Linux Tor Multiple vulnerabilities (GLSA 202107-25)
750726 OpenSUSE Security Update for tor (openSUSE-SU-2021:0926-1)

© [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](#)