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.torpr
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)

281839 Fedora Security Update for tor (FEDORA-2021-847ca2749a)

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)