TROVE

Last edited by **David Goulet** 2 months ago

TROVE: Tor Registry Of Vulnerabilities and Exposures

This page is an experimental registry of Tor software security problems, as we find them. We assign each one a number based on the year, ~~the month,~~ and an index.

For more information on the security policy we're using here, see the network team Security Policy page.

For high-severity issues not already publicly disclosed or being exploited, we will fix them in all affected releases, all at once, as soon as we can. We will notify the world that such a bug exists in advance of the patch, and we will release the patch once we believe it works.

TROVE ID	Ticket	Severity	Bug In	Fix In	Synopsis	CVE Id	Extra
TROVE-2016-10-001	tor#20384 (closed), tor#20894 (closed)	Medium	0.2.0.16-alpha	0.2.4,28, 0.2.5.13, 0.2.6.11 0.2.7.7, 0.2.8.9, 0.2.9.4-alpha	`buf_t` buffer read beyond end	CVE-2016-8860	(Debian: tracker DSA-3694 DLA-663-1) MEM
TROVE-2016-12-002	tor#21018 (closed)	Medium	0.2.0.8-alpha	0.2.4.28, 0.2.5.13, 0.2.6.11, 0.2.7.7, 0.2.8.12, 0.2.9.8 0.3.0.1-alpha	parse HS descs one byte past end	CVE-2016-1254	(Debian: tracker DSA-3741 DLA-754-1) MEM
TROVE-2017-001	tor#21278 (closed)	Medium	0.0.8pre1	0.2.4.28, 0.2.5.13, 0.2.6.11, 0.2.7.7, 0.2.8.13, 0.2.9.10, 0.3.0.4-rc,	Signed integer overflow when comparing versions		LL
TROVE-2017-002	tor#22253 (closed), tor#22246 (closed)	Medium	0.3.0.1-alpha	0.3.0.7, 0.3.1.1-alpha	Remotely triggerable assertion failure in relays		NULL
TROVE-2017-003	tor#22268 (closed)	Low	0.2.8.1-alpha	0.2.8.14, 0.2.9.11, 0.3.0.8, 0.3.1.3-alpha	Impersonation of ~~a single~~ a few fallback directory mirrors		initial post
TROVE-2017-004	tor#22493 (closed)	High	0.3.0.1-alpha	0.3.0.8, 0.3.1.3-alpha	Remote assertion failure against hidden services	CVE-2017-0375	(Debian: tracker)
TROVE-2017-005	tor#22494 (closed)	High	0.2.2.1-alpha	0.2.4.29, 0.2.5.14, 0.2.6.12, 0.2.7.8, 0.2.8.14, 0.2.9.11 0.3.0.8, 0.3.1.3-alpha	Remote assertion failure against hidden services	CVE-2017-0376	(Debian: tracker, #864424 DSA-3877 DLA-982-1))
TROVE-2017-006	tor#22753 (closed)	Medium	0.3.0.1-alpha	0.3.0.9, 0.3.1.4-alpha	Path selection issue	CVE-2017-0377	(Debian: tracker)
TROVE-2017-007	tor#22789 (closed)	Medium	0.2.3.8-alpha	0.3.0.10, 0.3.1.5-alpha, *0.2.5.15*, 0.2.8.15, 0.2.9.12	Remote assertion failure on openbsd		LIB

TROVE ID	Ticket	Severity	Bug In	Fix In	Synopsis	CVE Id	Extra
TROVE-2017-008	tor#23490 (closed)	Medium	0.2.7.2-alpha	0.2.8.15, 0.2.9.12, 0.3.0.11, 0.3.1.7	Stack disclosure in hidden services logs when SafeLogging disabled	CVE-2017-0380	(Debian: tracker, #876221) MEM
TROVE-2017-009	tor#24244 (closed)	Medium	0.2.4 and later	0.2.5.16, 0.2.8.17, 0.2.9.14, 0.3.0.13, 0.3.1.9, 0.3.2.6-alpha	Replay-cache ineffective for v2 onion services.	CVE-2017-8819	(Debian: tracker, DSA-4054)
TROVE-2017-010	tor#24245 (closed)	Medium	0.2.9 and later	0.2.9.14, 0.3.0.13, 0.3.1.9, 0.3.2.6-alpha	Remote DoS attack against directory authorities	CVE-2017-8820	(Debian: tracker, DSA-4054) NULL
TROVE-2017-011	tor#24246 (closed)	High	all Tor versions	0.2.5.16, 0.2.8.17, 0.2.9.14, 0.3.0.13, 0.3.1.9, 0.3.2.6-alpha	An attacker can make Tor ask for a password	CVE-2017-8821	(Debian: tracker, DSA-4054)
TROVE-2017-012	tor#24333 (closed)	Medium	0.2.5 and later	0.2.5.16, 0.2.8.17, 0.2.9.14, 0.3.0.13, 0.3.1.9, 0.3.2.6-alpha	Relays can pick themselves in a circuit path	CVE-2017-8822	(Debian: tracker, DSA-4054)
TROVE-2017-013	tor#24430 (closed)	High	0.2.7 and later	0.2.8.17, 0.2.9.14, 0.3.0.13, 0.3.1.9, 0.3.2.6-alpha	Use-after-free in onion service v2	CVE-2017-8823	(Debian: tracker, DSA-4054) MEM
TROVE-2018-001	tor#25074 (closed)	Medium	0.2.9.4-alpha	0.2.9.15, 0.3.1.10, 0.3.2.10, 0.3.3.3-alpha	Remote assertion failure in directory authority protocol handling	CVE-2018-0490	NULL
TROVE-2018-002	tor#25117 (closed)	Medium	0.3.2.1-alpha	0.3.2.10, 0.3.3.2-alpha	Use-after-free in KIST scheduler	CVE-2018-0491	MEM
TROVE-2018-003	tor#25250 (closed)	Low	0.3.3.1-alpha	0.3.3.3-alpha	Infinite loop in rust protover code	n/a	
TROVE-2018-004	tor#25251 (closed)	Low	0.2.9.4-alpha	0.2.9.15, 0.3.1.10, 0.3.2.10, 0.3.3.3-alpha	Crash on bad protocol information in consensus	n/a	NULL
TROVE-2018-005	tor#25517 (closed)	Medium/ Low	0.2.9.4-alpha	0.3.3.6, 0.3.4.2-alpha	Memory exhaustion against directory authorities	n/a	
TROVE-2018-006	tor#28630 (closed)	n/a	n/a	n/a	false alarm		
TROVE-2019-001	tor#29168 (closed)	Medium	0.3.2.1-alpha	0.3.3.12, 0.3.4.11, 0.3.5.8, 0.4.0.2-alpha	Remote memory exhaustion attack due to KIST ignoring outbuf highwater marks	CVE-2019-8955	

TROVE ID	Ticket	Severity	Bug In	Fix In	Synopsis	CVE Id	Extra
TROVE-2020-001	tor#33119 (closed)	Medium	0.3.5.1-alpha	0.3.5.11, 0.4.2.8, 0.4.3.6, 0.4.4.2-alpha	Remote crash against Tor built with NSS	CVE-2020-15572	MEM
TROVE-2020-002	tor#33120 (closed)	High	0.2.1.5-alpha	0.3.5.10, 0.4.1.9, 0.4.2.7, 0.4.3.3-alpha	Remote CPU-based denial of service	CVE-2020-10592	MEM
TROVE-2020-003	tor#33137 (closed)	Low	0.3.3.1-alpha	0.3.5.10, 0.4.1.9, 0.4.2.7, 0.4.3.3-alpha	Local crash, requires authenticated access to control port	n/a	ASSERT
TROVE-2020-004	tor#33619 (closed)	Medium	0.4.0.1-alpha	0.4.1.9, 0.4.2.7, 0.4.3.3-alpha	Remotely triggered memory leak	CVE-2020-10593	NULL?
TROVE-2020-005	tor#40080 (closed), tor#40086 (closed)	Medium	0.2.7.2-alpha	0.4.5.1-alpha, 0.4.4.6, 0.4.3.7, 0.3.5.12	Race condition allows extending over non-canonical connections		
TROVE-2021-001	tor#40304 (closed)	High	0.2.2.1-alpha	0.3.5.14, 0.4.4.8, 0.4.5.7, 0.4.6.1-alpha	CPU-based DoS from invalid directory data	CVE-2021-28089	MEM
TROVE-2021-002	tor#40316 (closed)	Medium	0.2.2.6-alpha	0.3.5.14, 0.4.4.8, 0.4.5.7, 0.4.6.1-alpha	Crash-based DoS, authorities only	CVE-2021-28090	MEM
TROVE-2021-003	tor#40389 (closed)	Medium	0.3.5.1-alpha	0.3.5.15, 0.4.4.9, 0.4.5.9, 0.4.6.5	Layer hint not validated on half-open streams	CVE-2021-34548	
TROVE-2021-004	tor#40390 (closed)	Low	0.2.8.1-alpha	0.3.5.15, 0.4.4.9, 0.4.5.9, 0.4.6.5	Incorrect error check on RAND_bytes	-	ERR
TROVE-2021-005	tor#40391 (closed)	Medium	0.2.4.4-alpha	0.3.5.15, 0.4.4.9, 0.4.5.9, 0.4.6.5	Hashtable-based DoS in circuit hashtable	CVE-2021-34549	HC
TROVE-2021-006	tor#40392 (closed)	High	0.3.0.1-alpha	0.3.5.15, 0.4.4.9, 0.4.5.9, 0.4.6.5	Out-of-bounds read in desc_decode_encryted_v3	CVE-2021-34550	MEM
TROVE-2021-007	tor#40446 (closed)	High	0.2.6.1-alpha	0.3.5.16, 0.4.5.10, 0.4.6.7	Batch/singleton crasher in ed25519-batch code	CVE-2021-38385	
TROVE-2021-008	tor#40474 (closed)	Low	0.4.5.8	0.4.5.11, 0.4.6.8, 0.4.7.2-alpha	v2 onion service metadata leak on disk	CVE-2021-22929	
TROVE-2021-009	tor#40538, tor#40539 (closed), tor#40674 (closed)	Medium	0.2.2.1-alpha	0.4.5.15, 0.4.7.11	DNS cache oracle		
TROVE-2022-001	tor#40626 (closed)	High	0.4.7.5-alpha	0.4.7.8	RTT estimation bug enables DoS		

TROVE ID	Ticket	Severity	Bug In	Fix In	Synopsis	CVE Id	Extra
TROVE-2022-002	tor#40730 (closed)	Medium	0.3.5.1-alpha	0.4.5.16, 0.4.7.13	SafeSocks option allows unsafe SOCKS	CVE-2023-23589	
TROVE-2023-001	arti#861 (closed)	Low	Arti 0.0.1	Arti 1.1.5	Arti: Local DoS via infinite loop in SOCKS code.		
TROVE-2023-002	arti#1000 (closed)	Low	Arti 1.1.0	Arti 1.1.8	Arti: bridgeless `bridges.enabled` configuration erroneously accepted.		
TROVE-2023-003	tor#40833 (closed)	Low	0.4.8.1-alpha	0.4.8.4	Buffer overrun in aarch64 HashX compiler		MEM
TROVE-2023-004	tor#40874	High	0.2.7.2-alpha	0.4.8.8	Remote triggerable assert on relays		
~~TROVE-2023-005~~	tor#40882	~~High~~					
TROVE-2023-006	tor#40883	High	0.4.8.1-alpha	0.4.8.9	Remote triggerable assert on onion services		
TROVE-2023-007							
TROVE-2024-001	arti#1269 (closed)	Low			DATA messages with len==0		
TROVE-2024-002	tpo/onion-services/onionspray#45 (closed)	High	before commit 187a94d934b20a25	1.6.0	Upstream HTTPS certificates not being validated		
TROVE-2024-003	arti#1409 (closed)	High	Arti 1.2.2	Arti 1.2.3, tor-circmgr 0.18.1	Arti: STUB circuits are too short (vanguards lite)	CVE-2024-35313	
TROVE-2024-004	arti#1400 (closed)	Medium	Arti 1.2.2	Arti 1.2.3, tor-circmgr 0.18.1	Arti: STUB circuits are used when STUB+ wanted, so too short (full vanguards)		
TROVE-2024-005	arti#1424 (closed)	High	Arti 1.2.3				
TROVE-2024-006	arti#1425 (closed)	Medium	Arti 1.2.3				
TROVE-2024-007	arti#1468 (closed)	Low	Arti 1.2.4		Timing variability in curve25519-dalek's Scalar29::sub/ Scalar52::sub		
TROVE-2024-008	arti#1474 (closed)	Low	Arti 1.2.4		Client rend circuits use the L3 vanguard as a rend point when full vanguards are enabled		
TROVE-2024-009	arti#1495 (closed)	Low	Arti 1.2.5		Undefined behavior in openssl's MemBio::get_buf		
TROVE-2024-010	arti#1627 (closed)	Medium	Arti		tor-socksproto usage can discard untimely data		
TROVE-2024-011	arti#1635 (closed)	Low? Medium?	Arti				
TROVE-2024-012	tor#40976	Low	-	-	RESERVED		

Remember: please get CVE-Ids for everything of severity Medium or higher. To get a CVE-Id, visit https://cveform.mitre.org/ .

MEM: Memory-safety issues. NULL: Null-pointer issues LL: Low-level implementation was incorrect. LIB: "Standard" library less specified than expected. ERR: Error handling api wasn't standardized. ASSERT: Bogus assertion. HC: Hashtable collision