

CVE-2026-45321

TanStack Unspecified Vulnerability

Exigent

CISA KEV since May 27, 2026

Actively exploited

Ransomware use known

On 2026-05-11, between approximately 19:20 and 19:26 UTC, 84 malicious versions across 42 @tanstack/* packages were published to the npm registry. The publishes were authenticated via the legitimate GitHub Actions OIDC trusted-publisher binding for TanStack/router, but the publish workflow itself was not modified. The attacker chained three known vulnerability classes — a pull_request_target "Pwn Request" misconfiguration, GitHub Actions cache poisoning across the fork↔base trust boundary, and runtime memory

EVRS

85/100

Immediate priority

CVSS V3.1

9.6

Critical · NVD

EPSS

0.011

64.1st percentile · FIRST

CISA DEADLINE

Jun 10, 2026

CISA federal deadline · Overdue by 4 months

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.011 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.6	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability could affect an open-source component, third-party library, protocol, or proprietary implementation that could be used by different products.

Basis: CISA KEV required action

extraction of the OIDC token from the Actions runner process — to publish credential-stealing malware under a trusted identity. Each affected package received exactly two malicious versions, published a few minutes apart.

Affected and fixed versions · GHSA-g7cv-rxg3-hmpx lists 76 more affected packages · 163 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
@tanstack/arktype-adapter	= 1.166.12	1.166.16	GitHub
@tanstack/eslint-plugin-router	= 1.161.9	1.161.13	GitHub
@tanstack/eslint-plugin-start	= 0.0.4	0.0.8	GitHub
@tanstack/history	= 1.161.9	1.161.13	GitHub
@tanstack/nitro-v2-vite-plugin	= 1.154.12	1.154.16	GitHub
@tanstack/react-router	= 1.169.5	1.169.9	GitHub
@tanstack/react-router-devtools	= 1.166.16	1.166.20	GitHub
@tanstack/react-router-ssr-query	= 1.166.15	1.166.19	GitHub

PACKAGE	AFFECTED	FIXED IN	SOURCE
tanstack\arktype-adapter	1.166.12 1.166.15	no fixed version listed	NVD
tanstack\eslint-plugin-router	1.161.9 1.161.12	no fixed version listed	NVD
tanstack\eslint-plugin-start	0.0.4 0.0.7	no fixed version listed	NVD
tanstack\history	1.161.9 1.161.12	no fixed version listed	NVD
tanstack\nitro-v2-vite-plugin	1.154.12 1.154.15	no fixed version listed	NVD
tanstack\react-router	1.169.5 1.169.8	no fixed version listed	NVD
tanstack\react-router-devtools	1.166.16 1.166.19	no fixed version listed	NVD
tanstack\react-router-ssr-query	1.166.15 1.166.18	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-g7cv-rxg3-hmpx

Additional guidance github.com/TanStack/router/security/advisories/GHSA-g7cv-rxg3-hmpx
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

NVD nvd.nist.gov/vuln/detail/CVE-2026-45321

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2026-29352

Current data evulnable.com/vulnerability-management/cve/CVE-2026-45321

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.