

CVE-2025-31125

Vite Vitejs Improper Access Control Vulnerability

CISA KEV since Jan 22, 2026

Actively exploited

Vite is a frontend tooling framework for javascript. Vite exposes content of non-allowed files using ?inline&import or ?raw? import. Only apps explicitly exposing the Vite dev server to the network (using --host or server.host config option) are affected. This vulnerability is fixed in 6.2.4, 6.1.3, 6.0.13, 5.4.16, and 4.5.11.

EVRS 77/100 Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.652 99.26th percentile · FIRST	CISA DEADLINE Feb 12, 2026 CISA federal deadline · Overdue by 8 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	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.652 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle 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

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
vite	< 4.5.11 ≥ 5.0.0 < 5.4.16 ≥ 6.0.0 < 6.0.13 ≥ 6.1.0 < 6.1.3 ≥ 6.2.0 < 6.2.4	4.5.11 · 5.4.16 · 6.0.13 · 6.1.3 · 6.2.4	NVD

Sources

Vendor guidance github.com/vitejs/vite/commit/59673137c45ac2bcfad1170d954347c1a17ab949

NVD nvd.nist.gov/vuln/detail/CVE-2025-31125

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-8866

Additional guidance github.com/vitejs/vite/security/advisories/GHSA-4r4m-qw57-chr8

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2025-31125

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