

CVE-2016-4523

Trihedral VTScada (formerly VTS) Denial-of-Service Vulnerability

CISA KEV since Apr 15, 2022

Actively exploited

The WAP interface in Trihedral VTScada (formerly VTS) 8.x through 11.x before 11.2.02 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via unspecified vectors.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.312 98.3rd percentile · FIRST	CISA DEADLINE May 6, 2022 KEV since 2022 · listed over a year
---	---------------------------------------	---	--

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	On the CISA KEV catalog for over two years
☒ EPSS	0.312 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 updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
vtscada	≥ 8.0.05 < 11.2.02	11.2.02	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-rp9v-r63v-9vfg	NVD	nvd.nist.gov/vuln/detail/CVE-2016-4523
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-5510
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-4523		

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