

CVE-2020-11899

Treck TCP/IP stack Out-of-Bounds Read Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

The Treck TCP/IP stack before 6.0.1.66 has an IPv6 Out-of-bounds Read.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 5.4 Medium · NVD	EPSS 0.184 97.2nd percentile · FIRST	CISA DEADLINE Mar 17, 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	0.184 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.4	☐ 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
tcp\ip	< 6.0.1.66	6.0.1.66	NVD
wyse 5050 all-in-one firmware	—	no fixed version listed	NVD
wyse 7030 firmware	—	no fixed version listed	NVD
wyse 5030 firmware	—	no fixed version listed	NVD
wyse 5050 all-in-one	—	no fixed version listed	NVD
wyse 7030	—	no fixed version listed	NVD
wyse 5030	—	no fixed version listed	NVD

Sources

Vendor guidance	treck.com	NVD	nvd.nist.gov/vuln/detail/CVE-2020-11899
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-4236
Current data	evulnable.com/vulnerability-management/cve/CVE-2020-11899		

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