

CVE-2019-20085

TVT NVMS-1000 Directory Traversal Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

TVT NVMS-1000 devices allow GET /. Directory Traversal

EVRS 83 / ₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.961 99.88th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · 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	0.961 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
nvms-1000 firmware	—	no fixed version listed	NVD
nvms-1000	—	no fixed version listed	NVD

Sources

Vendor guidance	exploit-db.com/exploits/47774	NVD	nvd.nist.gov/vuln/detail/CVE-2019-20085
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	europa.eu/enisa/eu-vulnerability/EUVD-2019-10641
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-20085		

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