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	CVSS V3.1	EPSS	CISA DEADLINE
83/100	7.5	0.961	May 3, 2022
Urgent priority	High · NVD	99.88th percentile · FIRST	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

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

Current data evulnable.com/vulnerability-management/cve/CVE-2019-20085

NVD nvd.nist.gov/vuln/detail/CVE-2019-20085

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2019-10641

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