

CVE-2025-48927

TeleMessage TM SGNL Initialization of a Resource with an Insecure Default Vulnerability

CISA KEV since Jul 1, 2025

Actively exploited

The TeleMessage service through 2025-05-05 configures Spring Boot Actuator with an exposed heap dump endpoint at a / heapdump URI, as exploited in the wild in May 2025.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 5.3 Medium · NVD	EPSS 0.111 95.9th percentile · FIRST	CISA DEADLINE Jul 22, 2025 KEV since 2025 · 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	Added to CISA KEV within the last two years
☒ EPSS	0.111 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source

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:** It is recommended that mitigations be applied per vendor instructions if available. If these instructions cannot be located or if mitigations are unavailable, discontinue use of the product
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
telemesssage	—	no fixed version listed	NVD

Sources

Vendor guidance	wired.com/story/how-the-signal-knock-off-app-telemesssage-got-hacked-in-20-minutes/	Additional guidance	cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2025-48927
NVD	nvd.nist.gov/vuln/detail/CVE-2025-48927	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-16207	Current data	evulnabile.com/vulnerability-management/cve/CVE-2025-48927

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