

CVE-2025-47729

TeleMessage TM SGNL Hidden Functionality Vulnerability

CISA KEV since May 12, 2025

Actively exploited

The TeleMessage archiving backend through 2025-05-05 holds cleartext copies of messages from TM SGNL (aka Archive Signal) app users, which is different functionality than described in the TeleMessage "End-to-End encryption from the mobile phone through to the corporate archive" documentation, as exploited in the wild in May 2025.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 4.9 Medium · NVD	EPSS 0.004 37.8th percentile · FIRST	CISA DEADLINE Jun 2, 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	0.004 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 4.9	☐ 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:** Apply mitigations per vendor instructions. Absent mitigating instructions from the vendor, discontinue use of the product
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
text message archiver	≤ 2025-05-05	after 2025-05-05	NVD

Sources

Vendor guidance	arstechnica.com/security/2025/05/signal-clone-used-by-trump-official-stops-operations-after-report-it-was-hacked/	Additional guidance	news.ycombinator.com/item?id=43909220
Additional guidance	theregister.com/2025/05/05/telemessage_investigating/	Additional guidance	cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2025-47729
NVD	nvd.nist.gov/vuln/detail/CVE-2025-47729	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-14003	Current data	evulnable.com/vulnerability-management/cve/CVE-2025-47729

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