

В США существуют клоны популярных мессенджеров и различных приложений для обмена сообщениями, которыми пользуются федеральные службы — полиция, ФБР и т.п. Одними из самых «ходовых» являются TM SGNL и TeleMessage — клоны мессенджеров Signal и Telegram. На эти клоны была осуществлена мощная хакерская атака, нацеленная на основные уязвимости.

Об этом сообщило Агентство по кибербезопасности и защите инфраструктуры США (CISA). Ведомство рекомендует немедленно установить исправления критических уязвимостей CVE-2025-48927, имеющих оценку CVSS 5,3 и позволяющих хакерам извлекать конфиденциальные данные из дампов памяти, которые становятся открытыми из-за неправильной конфигурации Spring Boot Actuator в приложении TeleMessage, открывающем конечную точку /heapdump. Похожие проблемы и с TM SGNL.

Федеральным службам CISA предоставило срок до 22 июля для применения необходимых исправлений. Агентство спешит, так как благодаря тем же хакерам был взломан «федеральный чат», откуда и так уже были утечки о ракетных ударах США по хуситам в Йемене.