# Basta uno sticker su Telegram per hackerarti! L'RCE critica da 9.8 è senza patch

*Di Carolina Vivianti 28/03/2026*

C'è qualcosa di profondamente inquietante in questa vulnerabilità: non serve cliccare, non serve aprire nulla. Basta ricevere. I ricercatori della Zero Day Initiative (ZDI) di Trend Micro hanno identificato una falla di tipo Remote Code Execution con punteggio CVSS 9.8 che colpisce Telegram su Android e Linux.

Il vettore è sorprendente nella sua banalità: sticker animati. File multimediali costruiti ad arte che, una volta recapitati, attivano automaticamente l'esecuzione di codice malevolo. Nessuna conferma, nessuna azione dell'utente. Il sistema li elabora per generare anteprime, ed è proprio lì che si consuma l'attacco.

Il risultato? L'attaccante può ottenere il controllo del dispositivo. Non parliamo solo di accesso superficiale: messaggi, contatti, sessioni attive. Tutto potenzialmente esposto. È una porta spalancata, e non è nemmeno visibile. L'allerta è stata diramata dallo CSIRT dell'Agenzia per la Cybersicurezza Italiana. La vulnerabilità è stata scoperta da Michael DePlante (@izobashi) of TrendAI Zero Day Initiative.
Prodotti colpiti e dettagli tecnici

Le versioni interessate sono chiare e circoscritte:

**Telegram per Android**

**Telegram per Linux**

Non si tratta di un bug marginale. La natura 0-click lo rende estremamente pericoloso, soprattutto in contesti dove la comunicazione è continua e automatizzata.

| Codice CVE | Severity | Sintesi |
|---|---|---|
| N/A | CVSS 9.8 | Esecuzione di codice remoto tramite sticker animati senza interazione |

Non sono stati forniti indicatori di compromissione (IoC), il che complica ulteriormente l'individuazione di eventuali attacchi già avvenuti.
Mitigazioni: tra compromessi e scelte drastiche

Qui le cose si fanno scomode. Le contromisure non sono eleganti, ma necessarie. Per gli utenti business, la prima linea di difesa è ridurre la superficie di attacco: limitare la ricezione di messaggi solo ai contatti fidati o utenti Premium. Una scelta che impatta la comunicazione, certo, ma riduce il rischio.

Per l'utenza generale, il discorso cambia. Le impostazioni di disattivazione del download automatico non bastano. Il parsing degli sticker avviene comunque, a livello di sistema. Quindi? Due opzioni. Nessuna perfetta: Disinstallare temporaneamente l'applicazione oppure utilizzare Telegram Web tramite browser aggiornati. La seconda soluzione sfrutta l'architettura sandbox dei browser moderni, che offre un livello di isolamento maggiore rispetto al client nativo. Non è una panacea, ma è meglio di niente.

Va però chiarito un punto che spesso sfugge quando si parla di vulnerabilità critiche. Nel contesto della Zero Day Initiative, gli exploit non circolano liberamente e non vengono trattati come merce da vendere al miglior offerente (ad es. broker zeroday o PSOA). Il programma impone regole precise: la scoperta viene gestita in modo responsabile, con processi di disclosure controllata e con l'obiettivo di arrivare a una correzione del problema (tramite la Coordinated Vulnerability Disclosure CVD).

È una dinamica molto diversa da quella dei mercati underground. Lì vulnerabilità di questo tipo possono diventare veri asset criminali, capaci di generare guadagni enormi. Exploit zero-click affidabili, soprattutto su piattaforme di comunicazione diffuse, possono valere milioni di euro nel circuito clandestino. Ed è proprio per evitare questo scenario che programmi come la Zero Day Initiative esistono: spostare queste scoperte dentro un perimetro regolamentato, dove il rischio viene gestito prima che finisca nelle mani sbagliate.