COMMUNITY CONTENT

Submit #781761: Dialogue Dialogue(ca.diagram.dialogue) 4.3.2 Segment Write Key Exposure

Title	Dialogue Dialogue(ca.diagram.dialogue) 4.3.2 Segment Write Key Exposure
Description	In the Android application ca.diagram.dialogue version 4.3.2, a hardcoded Segment write key was discovered in the source file res/raw/config.json. An attacker can extract this key through reverse engineering and use it to send arbitrary tracking events and modify user profiles via Segment's API. This allows injection of fraudulent analytics data, potentially leading to corrupted business intelligence, incorrect user segmentation, and misuse of downstream systems that rely on this data.
Source	⚠ https://www.notion.so/Segment-Write-Key-Exposure-Leading-to-Data-Injection-and-User-Profile-Manipulation-In-ca-diagram-dia-3262de3f97fb802fb5f0d2c9d179dcf6?source=copy_link
User	fxizenta (UID 28116)
Submission	03/17/2026 02:06 PM (17 days ago)
Moderation	04/03/2026 12:15 AM (16 days later)
Status	Accepted
VulDB entry	355043 [Dialogue App up to 4.3.2 on Android ca.diagram.dialogue config.json SEGMENT_WRITE_KEY hard-coded key]
Points	17

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling