VDB-355043 · CVE-2026-5455 · GCVE-100-355043

DIALOGUE APP UP TO 4.3.2 ON ANDROID CA.DIAGRAM.DIALOGUE CONFIG.JSON SEGMENT_WRITE_KEY HARD-CODED KEY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.0	$0-$5k	1.79

Summary

A vulnerability has been found in Dialogue App up to 4.3.2 on Android and classified as problematic. The impacted element is an unknown function of the file *file res/raw/config.json* of the component *ca.diagram.dialogue*. The manipulation of the argument *SEGMENT_WRITE_KEY* leads to hard-coded key. This vulnerability is listed as CVE-2026-5455. The attack must be carried out locally. In addition, an exploit is available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability, which was classified as problematic, has been found in Dialogue App up to 4.3.2 on Android. This issue affects an unknown part of the file *file res/raw/config.json* of the component *ca.diagram.dialogue*. The manipulation of the argument `SEGMENT_WRITE_KEY` with an unknown input leads to a hard-coded key vulnerability. Using CWE to declare the problem leads to CWE-321. The use of a hard-coded cryptographic key significantly increases the possibility that encrypted data may be recovered. Impacted is confidentiality.

It is possible to read the advisory at notion.so. The identification of this vulnerability is CVE-2026-5455. The exploitation is known to be easy. Attacking locally is a requirement. Technical details as well as a public exploit are known. The attack technique deployed by this issue is T1600.001 according to MITRE ATT&CK.

The exploit is available at notion.so. It is declared as proof-of-concept. The vendor was contacted early about this disclosure but did not respond in any way. By approaching the search of inurl:file res/raw/config.json it is possible to find vulnerable targets with Google Hacking.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

See VDB-351184, VDB-355041, VDB-355046 and VDB-355053 for similar entries.

Product

Type

- Android App Software

Name

- Dialogue App

Version

- 4.3.0
- 4.3.1
- 4.3.2

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 3.3
VulDB Meta Temp Score: 3.0

VulDB Base Score: 3.3
VulDB Temp Score: 3.0
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Hard-coded key
CWE: CWE-321 / CWE-320
CAPEC: 🔒
ATT&CK: 🔒

Physical: Partially
Local: Yes
Remote: No

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Google Hack: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

04/02/2026		VulDB entry created
04/03/2026	+0 days	Advisory disclosed
04/03/2026	+0 days	VulDB entry last update

Sources

Advisory: notion.so
Status: Not defined

CVE: CVE-2026-5455 (🔒)
GCVE (CVE): GCVE-0-2026-5455
GCVE (VulDB): GCVE-100-355043
scip Labs: https://www.scip.ch/en/?labs.20130704
See also: 🔒

Entry

Created: 04/03/2026 12:20 AM
Changes: 04/03/2026 12:20 AM (58)
Complete: 🔍
Submitter: fxizenta
Cache ID: 40:9D2:179

Submit

Accepted

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

Discussion

No comments yet. Languages: en.

Please log in to comment.