VDB-355041 · CVE-2026-5453 · EUVD-2026-18597

RICO SÓ VANTAGEM PRA INVESTIR APP UP TO 4.58.32.12421 ON ANDROID BR.COM.RICO.MOBILE SEGMENTSETTINGSMODULE.JAVA SEGMENT_WRITE_KEY HARD-CODED KEY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.0	$0-$5k	1.95-

Summary

A vulnerability, which was classified as problematic, has been found in Rico só vantagem pra investir App up to 4.58.32.12421 on Android. Impacted is an unknown function of the file *br/com/rico/mobile/di/SegmentSettingsModule.java* of the component *br.com.rico.mobile*. Performing a manipulation of the argument *SEGMENT_WRITE_KEY* results in hard-coded key. This vulnerability is identified as CVE-2026-5453. The attack is only possible with local access. Additionally, an exploit exists. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability classified as problematic has been found in Rico só vantagem pra investir App up to 4.58.32.12421 on Android. This affects an unknown functionality of the file *br/com/rico/mobile/di/SegmentSettingsModule.java* of the component *br.com.rico.mobile*. The manipulation of the argument `SEGMENT_WRITE_KEY` with an unknown input leads to a hard-coded key vulnerability. CWE is classifying the issue as CWE-321. The use of a hard-coded cryptographic key significantly increases the possibility that encrypted data may be recovered. This is going to have an impact on confidentiality.

The advisory is shared at notion.so. This vulnerability is uniquely identified as CVE-2026-5453. The exploitability is told to be easy. An attack has to be approached locally. Technical details and a public exploit are known. MITRE ATT&CK project uses the attack technique T1600.001 for this issue.

The exploit is shared for download 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.

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

The vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-18597). Entries connected to this vulnerability are available at VDB-351184, VDB-355043, VDB-355046 and VDB-355053.

Product

Type

- Android App Software

Vendor

- Rico

Name

- só vantagem pra investir App

Version

- 4.58.32.12421

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: 🔒
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-2026-5453 (🔒)
GCVE (CVE): GCVE-0-2026-5453
GCVE (VulDB): GCVE-100-355041
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20130704
See also: 🔒

Entry

Created: 04/03/2026 12:16 AM
Updated: 04/03/2026 12:18 PM
Changes: 04/03/2026 12:16 AM (59), 04/03/2026 12:18 PM (1)
Complete: 🔍
Submitter: fxizenta
Cache ID: 64:50F:179

Submit

Accepted

- Submit #781758: RICO.COM.VC Rico(br.com.rico.mobile) 4.58.32.12421 Segment Write Key Exposure (by fxizenta)

Discussion

No comments yet. Languages: en.

Please log in to comment.