VDB-355045 · CVE-2026-5457 · GCVE-100-355045

PROPERTYGURU AGENTNET SINGAPORE APP UP TO 23.7.10 ON ANDROID COM.ALLPROPERTY.ANDROID.AGENTNET BUILDCONFIG.JAVA SEGMENT_ANDROID_WRITE_KEY/SEGMENT_TOS_WRITE_KEY HARD-CODED KEY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.0	$0-$5k	1.73

Summary

A vulnerability was found in PropertyGuru AgentNet Singapore App up to 23.7.10 on Android. It has been classified as problematic. This impacts an unknown function of the file *com/allproperty/android/agentnet/BuildConfig.java* of the component *com.allproperty.android.agentnet*. This manipulation of the argument *SEGMENT_ANDROID_WRITE_KEY/SEGMENT_TOS_WRITE_KEY* causes hard-coded key. This vulnerability is registered as CVE-2026-5457. The attack needs to be launched locally. Furthermore, an exploit is available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability has been found in PropertyGuru AgentNet Singapore App up to 23.7.10 on Android and classified as problematic. Affected by this vulnerability is an unknown code block of the file *com/allproperty/android/agentnet/BuildConfig.java* of the component *com.allproperty.android.agentnet*. The manipulation of the argument `SEGMENT_ANDROID_WRITE_KEY/SEGMENT_TOS_WRITE_KEY` with an unknown input leads to a hard-coded key vulnerability. The CWE definition for the vulnerability is CWE-321. The use of a hard-coded cryptographic key significantly increases the possibility that encrypted data may be recovered. As an impact it is known to affect confidentiality.

The advisory is shared at notion.so. This vulnerability is known as CVE-2026-5457. The exploitation appears to be easy. An attack has to be approached locally. Technical details and also a public exploit are known. MITRE ATT&CK project uses the attack technique T1600.001 for this issue.

It is possible to download the exploit 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.

Product

Type

- Android App Software

Vendor

- PropertyGuru

Name

- AgentNet Singapore App

Version

- 23.7.0
- 23.7.1
- 23.7.2
- 23.7.3
- 23.7.4
- 23.7.5
- 23.7.6
- 23.7.7
- 23.7.8
- 23.7.9
- 23.7.10

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-2026-5457 (🔒)
GCVE (CVE): GCVE-0-2026-5457
GCVE (VulDB): GCVE-100-355045
scip Labs: https://www.scip.ch/en/?labs.20130704

Entry

Created: 04/03/2026 12:27 AM
Changes: 04/03/2026 12:27 AM (59)
Complete: 🔍

Submitter: fxizenta

Cache ID: 172:F24:179

Submit

Accepted

- Submit #781764: PropertyGuru AgentNet Singapore(com.allproperty.android.agentnet) 23.7.10 Segment Write Key Exposure (by fxizenta)

Discussion

No comments yet. Languages: en.

Please log in to comment.