VDB-355053 · CVE-2026-5462 · GCVE-100-355053

WAHOO FITNESS SYSTM APP UP TO 7.2.1 ON ANDROID COM.WAHOOFITNESS.SYSTM BUILDCONFIG.JAVA SEGMENT_WRITE_KEY HARD-CODED KEY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.0	$0-$5k	1.35

Summary

A vulnerability classified as problematic has been found in Wahoo Fitness SYSTM App up to 7.2.1 on Android. The affected element is an unknown function of the file *com/WahooFitness/SYSTM/BuildConfig.java* of the component *com.WahooFitness.SYSTM*. Performing a manipulation of the argument *SEGMENT_WRITE_KEY* results in hard-coded key. This vulnerability was named CVE-2026-5462. The attack needs to be approached 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, was found in Wahoo Fitness SYSTM App up to 7.2.1 on Android. This affects some unknown processing of the file *com/WahooFitness/SYSTM/BuildConfig.java* of the component *com.WahooFitness.SYSTM*. 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-2026-5462. 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.

See VDB-351184, VDB-355041, VDB-355043 and VDB-355046 for similar entries.

Product

Type

- Android App Software

Vendor

- Wahoo Fitness

Name

- SYSTM App

Version

- 7.2.0
- 7.2.1

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

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

Sources

Advisory: notion.so
Status: Not defined

CVE: CVE-2026-5462 (🔒)
GCVE (CVE): GCVE-0-2026-5462
GCVE (VulDB): GCVE-100-355053
scip Labs: https://www.scip.ch/en/?labs.20130704
See also: 🔒

Entry

Created: 04/03/2026 02:56 AM
Changes: 04/03/2026 02:56 AM (59)
Complete: 🔍
Submitter: fxizenta
Cache ID: 68:39C:179

Submit

Accepted

- Submit #781767: Wahoo Fitness Wahoo SYSTM(com.WahooFitness.SYSTM) 7.2.1 Segment Write Key Exposure (by fxizenta)

Discussion

No comments yet. Languages: en.

Please log in to comment.