VDB-355040 · CVE-2026-5452 · GCVE-100-355040

UCC CAMPUSCONNECT APP UP TO 14.3.5 ON ANDROID CAMPUSCONNECT.UCC BUILDCONFIG.JAVA HARD-CODED KEY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.0	$0-$5k	1.16

Summary

A vulnerability classified as problematic was found in UCC CampusConnect App up to 14.3.5 on Android. This issue affects some unknown processing of the file *campusconnect/BuildConfig.java* of the component *campusconnect.ucc*. Such manipulation leads to hard-coded key. This vulnerability is referenced as CVE-2026-5452. The attack can only be performed from a local environment. Furthermore, an exploit is available.

Details

A vulnerability was found in UCC CampusConnect App up to 14.3.5 on Android. It has been rated as problematic. Affected by this issue is an unknown function of the file *campusconnect/BuildConfig.java* of the component *campusconnect.ucc*. The manipulation 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.

The advisory is shared for download at notion.so. This vulnerability is handled as CVE-2026-5452. The exploitation is known to be easy. The attack needs to be approached locally. Technical details as well as a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1600.001.

The exploit is available at notion.so. It is declared as proof-of-concept.

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

- UCC

Name

- CampusConnect App

Version

- 14.3.0
- 14.3.1
- 14.3.2
- 14.3.3
- 14.3.4
- 14.3.5

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-2026-5452 (🔒)
GCVE (CVE): GCVE-0-2026-5452
GCVE (VulDB): GCVE-100-355040
scip Labs: https://www.scip.ch/en/?labs.20130704

Entry

Created: 04/03/2026 12:13 AM
Changes: 04/03/2026 12:13 AM (57)
Complete: 🔍
Submitter: fxizenta
Cache ID: 68:7B4:179

Submit

Accepted

- Submit #781757: CampusConnect™ UCC CampusConnect(campusconnect.ucc) 14.3.5 Uploadcare Private Key Exposure (by fxizenta)

Discussion

No comments yet. Languages: en.

Please log in to comment.