VDB-355044 · CVE-2026-5456 · GCVE-100-355044

ALIGN TECHNOLOGY MY INVISALIGN APP 3.12.4 ON ANDROID COM.ALIGNTECH.MYINVISALIGN.EMEA BUILDCONFIG.JAVA CDAACCESS_TOKEN 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 Align Technology My Invisalign App 3.12.4 on Android and classified as problematic. This affects an unknown function of the file *com/aligntech/myinvisalign/BuildConfig.java* of the component *com.aligntech.myinvisalign.emea*. The manipulation of the argument *CDAACCESS_TOKEN* results in hard-coded key. This vulnerability is cataloged as CVE-2026-5456. The attack must be initiated from a local position. Furthermore, there is an exploit 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 Align Technology My Invisalign App 3.12.4 on Android. Affected is an unknown code of the file *com/aligntech/myinvisalign/BuildConfig.java* of the component *com.aligntech.myinvisalign.emea*. The manipulation of the argument CDAACCESS_TOKEN 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 for download at notion.so. This vulnerability is traded as CVE-2026-5456. The exploitability is told to be easy. The attack needs to be approached locally. Technical details and a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1600.001.

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.

Product

Type

- Android App Software

Vendor

- Align Technology

Name

- My Invisalign App

Version

- 3.12.4

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-2026-5456 (🔒)
GCVE (CVE): GCVE-0-2026-5456
GCVE (VulDB): GCVE-100-355044
scip Labs: https://www.scip.ch/en/?labs.20130704

Entry

Created: 04/03/2026 12:25 AM
Changes: 04/03/2026 12:25 AM (59)
Complete: 🔍
Submitter: fxizenta
Cache ID: 68:313:179

Submit

Accepted

- Submit #781763: Align Technology My Invisalign(com.aligntech.myinvisalign.emea) 3.12.4 Contentful CDA Tokens Exposure (by fxizenta)

Discussion

No comments yet. Languages: en.

Please log in to comment.