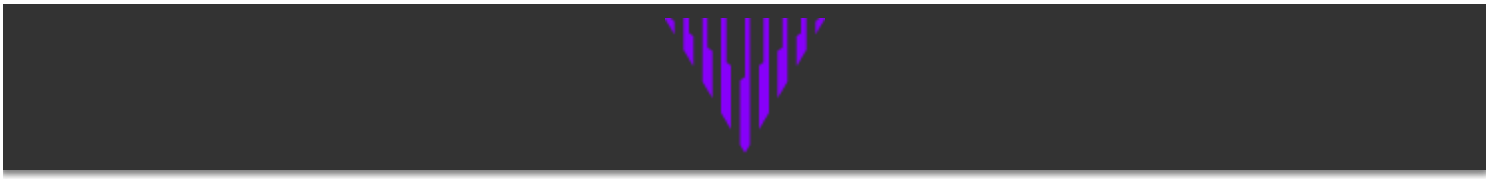

VDB-355046 · CVE-2026-5458 · EUVD-2026-18611

# NOELSE INDIVIDUALS & PRO APP UP TO 2.1.7 ON ANDROID COM.AFONE.NOELSE BUILDCONFIG.JAVA SEGMENT_WRITE_KEY HARD-CODED KEY

| CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score |
| --- | --- | --- |
| 3.0 | $0-$5k | 2.11- |

## Summary

A vulnerability was found in Noelse Individuals & Pro App up to 2.1.7 on Android. It has been declared as problematic. Affected is an unknown function of the file *com/reactnative/antelop/BuildConfig.java* of the component *com.afone.noelse*. Such manipulation of the argument *SEGMENT_WRITE_KEY* leads to hard-coded key. This vulnerability is documented as CVE-2026-5458. The attack needs to be performed locally. Additionally, an exploit exists. The vendor was contacted early about this disclosure but did not respond in any way.

## Details

A vulnerability was found in Noelse Individuals & Pro App up to 2.1.7 on Android and classified as problematic. Affected by this issue is some unknown processing of the file *com/reactnative/antelop/BuildConfig.java* of the component *com.afone.noelse*. The manipulation of the argument `SEGMENT_WRITE_KEY` 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 available at notion.so. This vulnerability is handled as CVE-2026-5458. The exploitation is known to be easy. Local access is required to approach this attack. Technical details as well as a public exploit are known. This vulnerability is assigned to T1600.001 by the MITRE ATT&CK project.

The exploit is available 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-2026-18611). Entries connected to this vulnerability are available at VDB-351184, VDB-355041, VDB-355043 and VDB-355053.

## Product

**Type**

- Android App Software

**Vendor**

- Noelse

**Name**

- Individuals & Pro App

**Version**

- 2.1.0
- 2.1.1
- 2.1.2
- 2.1.3
- 2.1.4
- 2.1.5
- 2.1.6
- 2.1.7

## 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-2026-5458 (🔒)
**GCVE (CVE)**: GCVE-0-2026-5458
**GCVE (VulDB)**: GCVE-100-355046
**EUVD**: 🔒
**scip Labs**: https://www.scip.ch/en/?labs.20130704
**See also**: 🔒

## Entry

**Created**: 04/03/2026 12:28 AM
**Updated**: 04/03/2026 12:18 PM
**Changes**: 04/03/2026 12:28 AM (59), 04/03/2026 12:18 PM (1)
**Complete**: 🔍
**Submitter**: fxizenta
**Cache ID**: 40:7B8:179

## Submit

**Accepted**

- Submit #781766: Noelse Noelse - Individuals & Pro(com.afone.noelse) 2.1.7 Segment Write Key Exposure (by fxizenta)

## Discussion

No comments yet. Languages: en.

Please log in to comment.