



SECURITY ASSESSMENT REPORT

Authorized Security Report

Prepared for the authorized owner of

example-customer.com

OVERALL RISK SCORE

10 /100



Safe, authorized simulation results

RISK LEVEL

Low

PACKAGE

Mobile Security

STATUS

Completed

FINDINGS

1

SCAN DATE

01 Aug 2026

REPORT TYPE

Client Evidence

Confidential security evidence

This report is intended for authorized stakeholders and contains safe passive assessment results.

Generated by BreakMesh

Executive Summary

This report summarises the findings from an automated security simulation performed by BreakMesh against <https://example-customer.com>. All checks are passive and safe-simulated — no destructive payloads are used. Overall result: grade **B** with a risk score of **10/100** and **Low** risk.

RISK SCORE	GRADE	RISK LEVEL	TOTAL FINDINGS
10/100	B	Low	1

SEVERITY	FINDINGS	RECOMMENDED ACTION
MEDIUM	1	Remediate within current sprint

Executive Actions

What passed: 0 checks completed without findings. What needs action: 1 checks produced findings for review.

Checks Performed

The **Mobile Security** package ran 1 checks. 0 completed without producing findings. Effectively tested 1 of 1 checks.

CHECK OUTCOME	COUNT	CHECKS
Passed	0	- No passing checks recorded
Needs review	1	- Mobile App Static Analysis (APK/IPA)

Scope & Confidence

Breakmesh is a continuous safeguard, not a guarantee of safety. This scan identifies and prioritises common, detectable weaknesses so they can be fixed before an attacker finds them — it reduces risk but cannot prove the absence of every vulnerability. No scanner can. Absence of findings means the checks that ran did not surface an issue, not that the target is immune to attack. Use these results as one layer of a defense-in-depth programme alongside secure development, timely patching, monitoring, and periodic human-led penetration testing.

SOC 2 Evidence Mapping

This mapping shows which SOC 2 trust service themes the completed checks can support as audit evidence.

SOC 2 THEME	MAPPED CHECKS	FINDINGS
Security	1	1
Confidentiality	1	1
Privacy	1	1

PCI-DSS v4.0 Control Mapping

This mapping shows which PCI-DSS v4.0 controls the completed checks can support as audit evidence.

CONTROL	MAPPED CHECKS	FINDINGS
1.2.1	8	
1.3.1	10	
11.3.1	20	
4.2.1	7	
6.2.4	48	
6.3.1	4	1
6.4.1	7	
7.2.1	28	
8.3.1	18	

ISO/IEC 27001:2022 Control Mapping

This mapping shows which ISO/IEC 27001:2022 controls the completed checks can support as audit evidence.

CONTROL	MAPPED CHECKS	FINDINGS
A.5.18	10	
A.5.24	3	
A.5.34	3	
A.8.14	7	
A.8.20	8	
A.8.24	7	
A.8.26	12	
A.8.28	30	
A.8.3	18	
A.8.5	18	
A.8.8	4	1
A.8.9	26	

HIPAA Security Rule Control Mapping

This mapping shows which HIPAA Security Rule controls the completed checks can support as audit evidence.

CONTROL	MAPPED CHECKS	FINDINGS
164.308(a)(1)	4	1
164.308(a)(6)	3	
164.308(a)(7)	7	
164.312(a)(1)	36	
164.312(c)(1)	36	
164.312(d)	18	
164.312(e)(1)	22	
164.502	3	

Detailed Findings

Hardcoded API Key in APK

MEDIUM

Static analysis of the uploaded APK found a hardcoded third-party API key string embedded in the compiled resources.

AFFECTED URLapp-release.apk

CONFIDENCEHigh

COMPLIANCE IMPACTSOC 2: Confidentiality, Privacy, Security
PCI-DSS v4.0: 6.3.1
ISO/IEC 27001:2022: A.8.8
HIPAA Security Rule: 164.308(a)(1)

REMEDIATIONMove API keys out of the client binary into a backend proxy or a runtime-fetched, scoped credential.

EVIDENCE**observed:** Static analysis of the uploaded APK found a hardcoded third-party API key string embedded in the compiled resources.

Scan ID: 8e3a434a-fa8c-54fb-b52b-423a9d2fd4a9 · This report is confidential and intended solely for the authorised owner of example-customer.com. Breakmesh performs passive simulation only. All findings should be validated by a qualified security professional prior to remediation.