PathCheck - GAEN-Mobile App - September 2020 Penetration Test Report

TARGET(S)

""

TEST PERIOD

Sep 29, 2020 → Oct 13, 2020

STATUS

Final

TEST PERFORMED BY

 Jana — Lead

 Arun S — Pentester

Contents

PDF created Oct 23, 2020 21:11 UTC
Cobalt Web App 2020
by Cobalt Labs • San Francisco, CA •
cobalt.io

Executive Summary

A gray box penetration test of the PathCheck - GAEN-Mobile App mobile application was conducted in order to assess its risk posture and identify security issues that could negatively affect PathCheck's data, systems, or reputation. The scope of the assessment covered PathCheck gaen-mobile External iOS Beta version 1378 and PathCheck gaen-mobile Google Alpha Closed 1.0.3. The pentest was conducted by 2 pentester(s) between Sep 29, 2020 and Oct 13, 2020.

This penetration test was a manual assessment of the security of the application's functionality, business logic, and vulnerabilities such as those catalogued in the OWASP Top 10. The assessment also included a review of security controls and requirements listed in the OWASP Mobile Application Security Verification Standard (MASVS). The pentesters leveraged tools to facilitate their work; however, the majority of the assessment involves manual analysis.

The pentesters identified 0 High, 0 Medium, and 2 Low risk vulnerabilities.

Overall, the pentesters found that the application exhibits a good security posture during the assessment. The application is well built, with many security best practices in place. No major issues were discovered during the test because of this. One of the reported issues involves the lack of SSL Pinning allowing attackers to potentially launch a Man-In-The-Middle attack. The other issue related to the lack of root detection mechanism which could allow an attacker with local access to the deice to steal data or interact with the application in an unintended fashion. Both findings are considered Low severity.

Significant findings include:

- Lack of SSL Pinning
- Lack of Root Detection Mechanism

Specific recommendations are provided for each finding. As a whole, the recommendations indicate gaps that can be addressed by configuring SSL pinning as well as implementing checks which can detect if the mobile application is running on a rooted/ jailbroken device.

Methodology

The test was done according to penetration testing best practices. The flow from start to finish is listed below.

Pre Engagement

- Scoping
- Customer
- Documentation
- Information
- Discovery

Penetration Testing

- Tool assisted assessment
- Manual assessment
- Exploitation
- Risk analysis
- Reporting

Post Engagement

- Prioritized remediation
- Best practice support
- Re-testing

PDF created Oct 23, 2020 21:11 UTC
Cobalt Web App 2020
by Cobalt Labs • San Francisco, CA •
cobalt.io

Risk Factors

Each finding is assigned two factors to measure its risk. Factors are measured on a scale of 1 (very low) through 5 (very high).

Impact

This indicates the finding's effect on technical and business operations. It covers aspects such as the confidentiality, integrity, and availability of data or systems; and financial or reputational loss.

Likelihood

This indicates the finding's potential for exploitation. It takes into account aspects such as skill level required of an attacker and relative ease of exploitation.

PDF created Oct 23, 2020 21:11 UTC
Cobalt Web App 2020
by Cobalt Labs • San Francisco, CA •
cobalt.io

Criticality Definitions

Findings are grouped into three criticality levels based on their risk as calculated by their business impact and likelihood of occurrence, `risk = impact * likelihood`. This follows the OWASP Risk Rating Methodology.

High

Vulnerabilities with a high or greater business impact and high or greater likelihood are considered High severity. Risk score minimum 16.

Medium

Vulnerabilities with a medium business impact and likelihood are considered Medium severity. This also includes vulnerabilities that have either very high business impact combined with a low likelihood or have a low business impact combined with a very high likelihood. Risk score between 5 and 15.

Low

Vulnerabilities that have either a very low business impact, maximum high likelihood, or very low likelihood, maximum high business impact, are considered Low severity. Also, vulnerabilities where both business impact and likelihood are low are considered Low severity. Risk score 1 through 4.

Terms

Please note that it is impossible to test networks, information systems and people for every potential security vulnerability. This report does not form a guarantee that your assets are secure from all threats. The tests performed and their resulting issues are only from the point of view of Cobalt Labs. Cobalt Labs is unable to ensure or guarantee that your assets are completely safe from every form of attack. With the ever-changing environment of information technology, tests performed will exclude vulnerabilities in software or systems that are unknown at the time of the penetration test.

PDF created Oct 23, 2020 21:11 UTC
Cobalt Web App 2020
by Cobalt Labs • San Francisco, CA •
cobalt.io