

November 23, 2020

PathCheck Foundation
955 Massachusetts Avenue
Suite 213
Cambridge, MA 02139

Tuik Security Group LLC (Tuik) performs and facilitates numerous security testing activities for PathCheck Foundation's (PathCheck) GAEN-mobile application. The GAEN-mobile application undergoes rigorous security testing supported by industry leaders including Cobalt.io, best-of-breed tools including Veracode and WhiteSource, opensource testing solutions including the Mobile Security Framework, certified penetration testing experts, along with numerous volunteers reviewing and testing the GAEN-mobile application. Google, Apple, and PathCheck use the BugCrowd crowdsourced cybersecurity platform to continually assess risk, find critical issues faster, and maintain security best practices within the GAEN-mobile application.



Security testing includes ongoing Binary Static Code Analysis, Software Composition Analysis, Dynamic Application Security Testing, and Timeboxed Integral Penetration-testing to thoroughly assess the application's security and locate any vulnerabilities that could impact the confidentiality, integrity, or availability of the GAEN-mobile ecosystem. The multifaceted risk assessment approach analyzes PathCheck's defense-in-depth strategy to provide a comprehensive technical risk assessment, as no single type of testing can discover all possible software flaws and vulnerabilities.

The approach follows leading industry best practices, standards, and methodologies incorporating elements from several established testing models, including:

- National Institute of Standards and Technology 800-115 (NIST)
- ISO 27001 Information Security Management System (ISMS)
- Penetration Testing Execution Standard (PTES)
- Federal Risk and Authorization Management Program (FedRAMP) Penetration Test Guidance
- Open Source Security Testing Methodology Manual (OSSTMM)
- Open Web Application Security Project (OWASP) – Penetration Testing Resources
- Payment Card Industry Data Security Standard (PCI DSS) – Penetration Testing Guidance

For any security issue identified, PathCheck works swiftly to remediate the issue and, when provided, PathCheck follows Google and Apple's remediation guidance.

At present, there are zero vulnerabilities that directly impact the confidentiality, integrity, or availability of the GAEN-mobile ecosystem.

Respectfully,



Alexander Chaveriat
Chief Innovation Officer