WhiteHat Sentinel Mobile SE

Mobile Application Security

Mobile devices have dramatically changed the way business is conducted. Enterprises are building and supporting an increasing number of mobile applications. This development process features an accelerated lifecycle, with little time between design and production. Web app security is a mature process, but one that does not always translate well to mobile app development. Mobile application security requires new testing tools and approaches; not on emulators, but on physical devices in real-world attack scenarios.

WhiteHat Sentinel Mobile Standard Edition (SE) identifies vulnerabilities within mobile applications created internally or by third-party agencies via binaries, helping create a secure ecosystem for organizations and users alike. Every vulnerability finding is verified by our Threat Research Center (TRC) to curate the results for nearly zero false positives.

WhiteHat Sentinel Mobile SE represents cutting-edge mobile application security testing. Mobile SE employs a combination of tools, processes, and expertise to deliver vulnerability management solutions in line with the guidelines of the OWASP Mobile Security Project.

Sentinel Mobile SE Features

- Supports both iOS (Objective C) and Android (Java)
- Device-based, fully automated testing
- Used for all developer-signed binaries; does not require source code
- Detailed reporting with results and verified, prioritized findings
- Configuration-related checks
- Data transmission-related checks
- Provides detailed descriptions of vulnerabilities and offers remediation guidance
- Ask a Question feature allows you to learn more from our TRC team about each vulnerability
- Unlimited testing for a year
- All results available in Sentinel

WhiteHat Sentinel Mobile SE Benefits

Align mobile security strategy

Review critical mobile applications to achieve a Big Picture view of your organization's application security posture.

Obtain verified, actionable results with near zero false positives

Our TRC validates every potential vulnerability so you can focus your remediation efforts on verified bugs and defects and save resources.

Identify security issues and vulnerabilities in mobile application binaries

We provide a breakdown of all third-party libraries being used in the source code; their vulnerabilities, licensing, and quality details.

Experience direct access to a dedicated team of security expertise

Access TRC engineers via Sentinel to ask questions regarding vulnerabilities and obtain remediation guidance.

WHITEHAT THREAT RESEARCH CENTER:

WhiteHat Security's TRC is an elite team of security industry experts. The TRC is an integral component of the WhiteHat Sentinel™ Product Family, and an extension of your mobile development team.

Vulnerabilities identified by NowSecure tools and other proprietary algorithms in the Sentinel platform are verified by experts of the TRC using the latest techniques in mobile forensic discovery and security intelligence to ensure that you get actionable, confirmed results and near-zero false positives.

With the WhiteHat Security Index, you can know your security score across all your web and mobile applications to help manage your risk and allocate development resources with greater accuracy.

Mobile SE Functionality Map

FEATURES AND CHECKS	
Code Obfuscation / encryption	Dynamic code downloading
Application Certification	Arbitrary code execution
Dynamic code loading / decompiling	Root execution
Improper SSL/TLS, SSL downgrade, enforcement	World-writable / -readable files
Sensitive data leakage	.ZIP files
Arbitrary file writing	Interprocess Communication