SCANTIST

Binary Vulnerability Analysis

Scan for vulnerabilities in binary programs without a need for source code

Binary-Level Analysis

Our tools scan applications at the binary level, ensuring that we uncover vulnerabilities introduced not only during development but also from compilation.

Efficient Dual Engines for Static Analysis

Our unique static analysis utilizes both existing vulnerability signatures and metrics to efficiently detect vulnerable functions. Meanwhile, cross-platform vulnerability-oriented dynamic detection is used to discover the vulnerability trigger input.

Cross-Platform, Cross-Architecture Support

Our scanning technology supports multiple platforms and architectures. So be it C/C++, Windows/Linux, or Intel (x86/x64)/ARM, our vulnerability analysis can be carried out on a wide-range of applications.

Extensive Coverage

Our tools are built to maximize coverage, ensuring every critical component of your application is analyzed. Furthermore, our analysis extends to cover not just your application, but also third-party dependencies that it might have.

Detailed and Actionable Reports

Vulnerability analysis is incomplete without a report that is not only detailed, but also actionable. Our team provides you with accurate information and support to better secure your application after the analysis.

Scantist scans applications for a wide-range of memory-safety related vulnerabilities like stack/heap overflow, out-of-bounds access, use-after-free and other memory corruptions.

SCANTIST

Managed Services

Choose from our Basic and Enhanced service options based on your needs.

Basic Analysis

Static Analysis Only

Dual-engine based static analysis: (1) Signature based vulnerability matching[1] with 20000 signatures, (2) metrics based accurate vulnerability location

Suitable for applications running in specialized environments using custom hardware

Scales to any binary, allowing analysis of large, complex code-base as required

Enhanced Analysis

Static and Dynamic Analysis

In addition to duel-engine based static analysis, providing runtime dynamic vulnerability analysis[2] on binary code

Suitable for mission-critical applications running in widely-used environments

Comprehensive vulnerability report, including confirmative input triggers

Post-analysis support from our security team

[1]Our binary vulnerabilities signature database covers about 10,000 key CVEs and 100 key OSS projects (Linux kernel, OpenSSL, Google Android, Google Chromium, Firefox, FreeBSD, Apache Http Sever, QEMU, Libxml2).

[2]Dynamic analysis discovers zero-day memory corruption vulnerabilities, including stack/heap overflow, out-of-bounds read/write, use-after-free, double-free, uninitialized reference, and type confusion vulnerabilities.

	Platforms			Architectures (* 32/64-Bit)				Languages		
				Intel*	ARM*	MIPS	PowerPC	C/C++	Obj-C	Java
Static Analysis	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic Analysis	✓	✓	✓	✓	✓	✓	–	✓	–	–

We are continuously adding support for new platforms, architectures and languages

About Scantist

Scantist is a cyber-security spin-off from Nanyang Technological University, Singapore. We provide vulnerability detection services to enterprise clients, helping build a global cyber-secure society.

Website : www.scantist.com
Email : contact@scantist.com

The efficacy of Scantist's approach can be validated by the 100+ CVEs awarded to the company, of which 35 were awarded in the last one year alone.