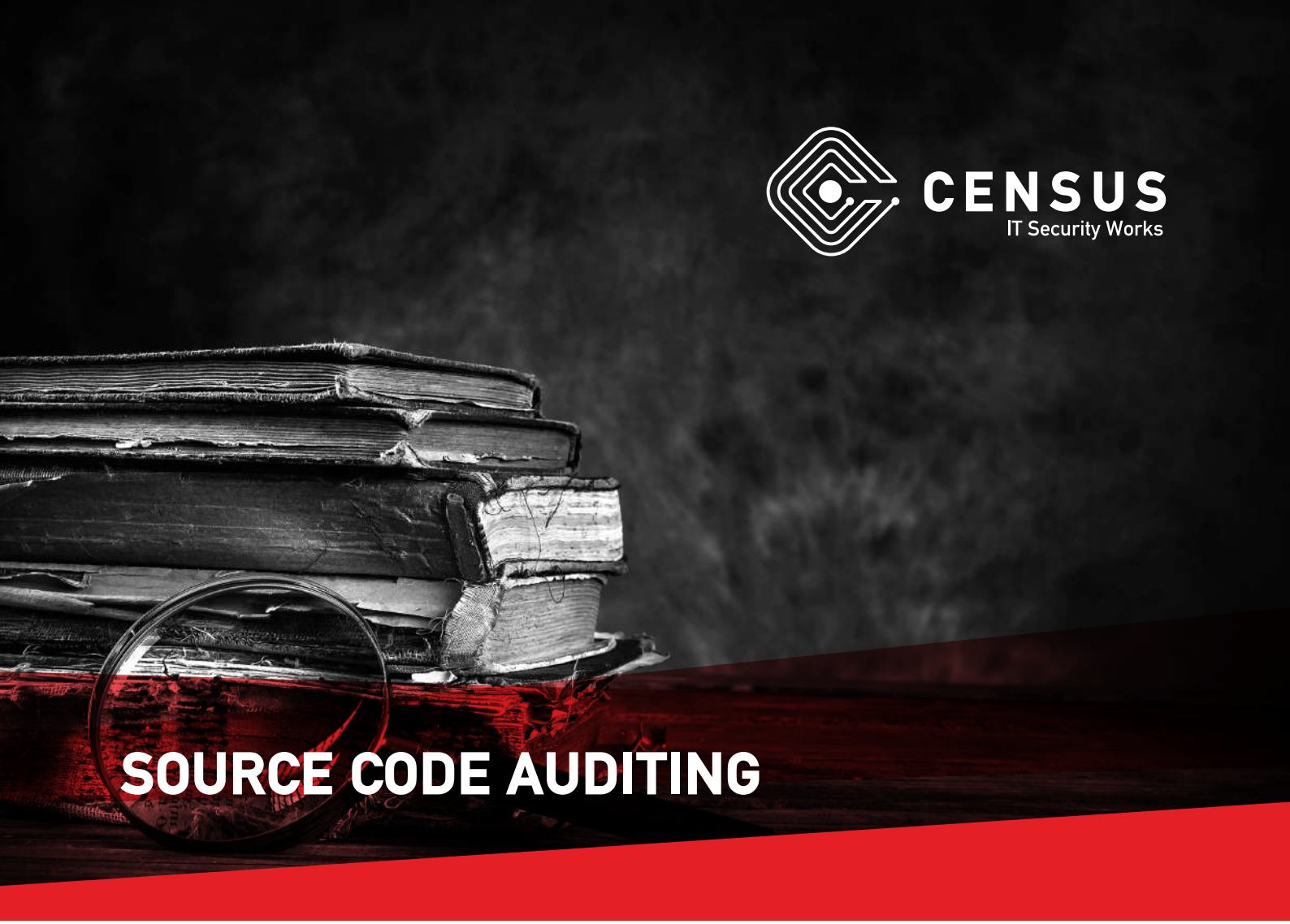
CENSUS
IT Security Works



SOURCE CODE AUDITING

WHAT IS SOURCE CODE AUDITING?

Source Code Auditing is an assessment process that identifies security issues in software projects by examining the project's source code line-by-line. Source Code Auditing can be applied to any type of software (systems software, application libraries, web applications, mobile applications etc.). It is capable of identifying all types of security issues and provides the best possible assessment coverage during the security analysis of a software module.

WHEN IS SOURCE CODE AUDITING APPROPRIATE?

Source Code Auditing can help identify security issues during the **development phase** of a software project. In this way, it effectively minimizes any post-release risks and supports the production of high quality products. Auditing can be applied to a complete software module that is in release candidate status or to a specific functionality that has reached a certain milestone (e.g. auditing of a software patch). Source Code Auditing can also be applied to acquired **third party** code. In this case, the acquiring organization applies Source Code Auditing to eliminate any risks introduced by the third party codebase.

CENSUS SOURCE CODE AUDITING SERVICES

CENSUS provides advanced Source Code Auditing services, based on years of professional experience and focused research in the area of Software Security. Through Source Code Auditing, CENSUS supports the Secure Software Development Life Cycle of major corporations around the world, identifying security vulnerabilities in a wide set of applications, ranging from e-banking systems and mobile payment apps, to cloud and embedded systems software components.

The Source Code Auditing services cover software implemented in the following programming languages: C, C++, Objective C, Go, Java, C#, PHP, Python, Perl, Ruby, Swift, JavaScript, Visual Basic, ASP, x86 / x64 Assembly, Unix Shell Scripting, Fortran and Cobol.

For vulnerabilities found in commonly used third party code, CENSUS releases public advisories and works with vendors (following a responsible disclosure procedure), so that end-users may be protected as early as possible from the security risks involved. Some of these advisories are presented below:

- "Linux kernel SUNRPC off-by-two buffer overflow", 2009
- "CoreHTTP web server off-by-one buffer overflow vulnerability", 2009
- "FreeBSD kernel NFS client local vulnerabilites", 2010
- "libpurple OTR information leakage", 2012

METHODOLOGY

The CENSUS Source Code Auditing service has been designed to meet the needs of modern Software Development Life Cycle (SDLC) strategies. The service introduces the necessary auditing controls so that the development conforms to the Secure SDLC paradigm, while in Agile Development environments it becomes part of the standard testing procedure by integrating with the established processes and tools.

The auditing procedure followed involves the manual line-by-line analysis (static analysis) of the project's source code by security experts. When a live testing environment is available, functional testing (dynamic analysis) is also performed, in order to quickly evaluate complex issues that were identified through the line-by-line analysis.

CENSUS experts go well beyond the identification of standard issues (e.g. OWASP Top 10 issues), identifying security defects that may be unique to the business logic of the investigated application or defects that may appear due to the use of an application within a specific environment setting (e.g. execution of app under specific OS version).

The auditing procedure can be extended to include a review of the build process, the released software package and its default configuration, to identify defects (such as the misconfiguration of security controls) introduced during the software building / packaging stage.

Deliverables can either be in the form of a technical report or an issue tracker spreadsheet based on a client selected scoring system (e.g. CVSS 2.0). Both report and tracker describe the identified security vulnerabilities in detail, evaluate their respective risks and propose mitigations for these risks. Issues can also be documented on a bug reporting system designated by the client.

CENSUS experts remain at the client's service for issue retesting and consulting regarding the handling of open issues.

BENEFITS

Source Code Auditing plays a crucial part in the delivery of higher quality software. It is the only assessment method that is capable of identifying all types of security vulnerabilities and its white-box assessment methodology makes it unique in that it can quickly uncover architectural flaws that could lead to multiple security vulnerabilities later on in the development of the project.

Experience has shown that the close interaction between developers and source code auditors raises the development team's awareness level on security issues and leads to the output of more robust code on each development sprint.

Finally, it is a well established fact that fixing a security vulnerability after an application's release, comes with an increased cost to software vendors, both in terms of business and development. Source Code Auditing helps in minimizing these costs, by identifying and addressing security issues early on in the software development process.

For more information about the CENSUS Source Code Auditing services please visit: **www.census-labs.com**

CENSUS
IT Security Works

www.census-labs.com

USA
607 Boylston Street,
Suite 165L, Boston, MA 02116
T. +1 617-448-5050
E. usa@census-labs.com

EUROPE
128, Leoforos Andrea Syggrou,
11745, Athens, Greece
T. +30 210 220 8989-90
E. eu@census-labs.com

UK
4th floor, The Pinnacle,
Station Way, Crawley RH10 1JH
T. +44 (0) 1293 763 336
E. uk@census-labs.com