Oracle Software Security Assurance

Oracle's methodology for the development and maintenance of security in its products

As organizations increasingly rely on software controls to protect their computing environments and data, ensuring that these controls operate in the way they were intended has become a paramount concern. Software security assurance encompasses all the activities involved in ensuring that software operates at an expected and predictable level of security. Managing security incidents, meeting complex regulatory and auditing requirements, and keeping current with security releases can add tremendous costs to an organization's IT budget; thus organizations must give careful consideration to how their software providers approach software security assurance.

Security built in, not bolted on

Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance is Oracle's methodology for building security into the design, build, testing, delivery, and maintenance of its products. Oracle's goal is to ensure that Oracle's products, as well as the customer systems that leverage those products, remain as secure as possible.

Secure Coding Standards

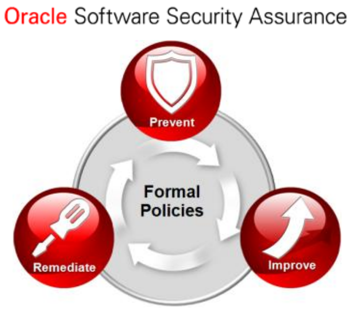
Secure software does not happen by itself. It requires consistently applied methodologies across each organization; methodologies that conform to stated policies, objectives, and principles.

Oracle Secure Coding Standards are a guide for developers in their efforts to produce secure code. The standards discuss general security knowledge areas such as design principles and common vulnerabilities, and provide specific guidance on topics such as data validation, data privacy, user management, and more.

All Oracle developers are required to be familiar with these standards and apply them when designing and building products. The coding standards have been developed over many years and incorporate best practices as well as lessons learned from continued vulnerability testing by Oracle's internal ethical hacking team. Oracle ensures that developers are familiar with its coding standards by requiring that they undergo secure coding training. The Secure Coding Standards are a key component of Oracle Software Security Assurance and adherence to the Standards is assessed and validated throughout the useful life of all Oracle products.

Comprehensive Security Analysis and Testing

Security testing at Oracle includes both functional and non-functional activities for



STATIC CODE ANALYSIS

Static security analysis of source code is used during the entire product development cycle. This type of analysis works very well for identifying buffer overflows and memory leaks in C/C++ code, resource handling issues in J2EE and .NET, finding improper credentials handling, various injections, incorrect system configurations, etc.

DYNAMIC CODE ANALYSIS

Dynamic analysis activity always takes place during latter phases of product development. Dynamic analysis is aimed at externally visible product interfaces and APIs and frequently relies on specialized tools for testing. Both manual and automatic tools are used for testing. Automatic tools employ fuzzing techniques to test network-accessible product interfaces and protocols, while manual tools require making the modifications by hand, but allow for much greater accuracy and precision.

verification of product features and quality. Although these types of tests often target overlapping product features, they have different goals and so are carried out by different teams. Functional and non-functional security tests complement each other to provide comprehensive security coverage of Oracle.

Functional security testing is typically executed by regular product QA teams as part of normal product testing cycle. During this testing, QA engineers verify conformance of implemented security features to what had been previously agreed upon in the functional specifications during the architectural and checklist review process.

Non-functional security analysis and testing verify the security assurance of Oracle products, including the identification and remediation of vulnerabilities and resistance to attacks. There are two broad categories of tests employed for testing Oracle products: static and dynamic analysis. These tests fit differently in the product development lifecycle and tend to find different categories of issues, so they are used together by Oracle security teams.

Security vulnerability handling and remediation

The Critical Patch Update program is the primary mechanism for the release of security bug fixes for Oracle products. Critical Patch Updates are released quarterly on the Tuesday closest to the 17th of the month in January, April, July, and October. In addition, Oracle retains the ability to issue out of schedule patches or workaround instructions in case of particularly critical vulnerabilities and/or when active exploits are reported "in the wild." This program is known as the Security Alert program.

Oracle’s security vulnerability handling and remediation procedures are intended to provide customers with the following benefits:

- Maximum Security—Vulnerabilities are remediated by Oracle in order of severity. This process ensures that the most critical security holes are patched first in the Critical Patch Update, thereby optimizing the security posture of all Oracle customers.
- Lower Administration Costs—A fixed security patching schedule takes the guesswork out of patch management. The schedule is also designed to avoid typical "blackout dates" during which customers cannot typically alter their production environments. The coordination of the release of the fixes across the Oracle stack also results from Oracle’s focus on testing the fixes across various dependent products, thus reducing your testing effort and associated costs.
- Simplified Patch Management—Patch updates are cumulative for most Oracle products. This provides customers the ability to quickly "catch up" to the current security release level, since the application of the latest cumulative Critical Patch Update resolves all previously addressed vulnerabilities.

Disclaimer: Please note that the relevant contract between you and Oracle determine the legal terms and conditions applicable to the products and/or services acquired. *This information is provided on an “AS-IS” basis without warranty and is subject to change.* It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.

> *“The permeation of information technology into virtually every aspect of our lives has been met by an exponential increase in IT-based attacks and attackers. Far too many of them are successful, and result from preventable security weaknesses. It is therefore imperative that all Oracle products and services be designed, developed and delivered to be secure - which is the purpose of Oracle Security Software Assurance”*
>
> **MARY ANN DAVIDSON**
> CHIEF SECURITY OFFICER
> ORACLE CORPORATION

For more information

The Oracle Software Security Assurance web site is located at http://www.oracle.com/us/support/assurance.

CONNECT WITH US

blogs.oracle.com/security
facebook.com/oracle
twitter.com/oracle
oracle.com

FOR MORE INFORMATION
Contact: 1.800.ORACLE1