May 09, 2018

Veracode, Inc.
65 Network Drive
Burlington, MA 01803
United States

Michael Ambrus
5559 Eureka Dr Ste B
Hamilton, OH 45011-4267
United States

To whom it may concern:

This letter summarizes activities performed by Veracode in assessing the security posture of the **UltraCompare** application.

Veracode is the only independent provider of cloud-based application security verification and intelligence services delivering unbiased proof of application security to stakeholders across the software supply chain. The Veracode platform provides the fastest, and most comprehensive solution for improving the security of internally developed, purchased or outsourced software applications and third-party components. Offered as a Software-as-a-Service (SaaS), Veracode uses its award-winning, proprietary *static* and *dynamic* analysis technologies to test software applications for security flaws and vulnerabilities, reporting detailed actionable findings and remediation guidance.

Veracode's patented *static binary analysis* technology inspects software executables (compiled binaries or bytecode) for security flaws without requiring customers to provide their intellectual property in the form of source code. By examining a compiled form of an application, static binary analysis can provide a more comprehensive picture of real-world vulnerabilities with a lower false positive rate. Through advanced modeling, Veracode's static engine detects flaws in the software's inputs and outputs that cannot be seen through penetration testing alone. Specifically, Veracode's binary analysis creates a behavioral model by analyzing an application's control and data flow through executable machine code - the way an attacker sees it. Unlike source code review tools, this approach accurately detects issues in the core application and extends coverage to vulnerabilities found in 3rd party libraries, pre-packaged components, and code introduced by compiler or platform-specific interpretations. Binary analysis can also detect other threats, such as those coming from malicious code and backdoors – which are difficult to spot with traditional tools because they are not visible in source code.

Veracode also employs advanced *dynamic analysis* techniques to test the application for security vulnerabilities. Dynamic analysis consists of two primary phases: the 'spider' phase: which enumerates all exposed functionality and catalogues the available attack surfaces; and the 'attack' phase: which submits specially crafted requests in an effort to trigger application behavior that would indicate the presence of exploitable security vulnerabilities. The Veracode dynamic analysis service is a highly evolved, next generation dynamic scanning technology. It is designed for thoroughness, in that it addresses assessment coverage and accuracy limitations prevalent in existing dynamic scanning approaches that have seen little change since their introduction over a decade ago. Unlike its predecessors, Veracode's dynamic engine is designed for next generation websites, including advanced support for both the latest Web 2.0 technology (including JavaScript, AJAX and basic flash support) and sophisticated authentication schemes employed by leading online platforms. Veracode has built it from the ground up to support the SaaS model, providing on-demand dynamic analysis launched from the Veracode platform.

Through automated analysis, Veracode tests to determine the presence of common application vulnerabilities, such as those as defined by the current SANS Top 25 and OWASP Top 10. For example, the OWASP Top 10 includes the following flaw categories:

A1: Injection Flaws
A2: Cross Site Scripting (XSS)
A3: Broken Authentication and Session Management
A4: Insecure Direct Object Reference
A5: Cross Site Request Forgery (CSRF)
A6: Security Misconfiguration
A7: Insecure Cryptographic Storage
A8: Failure to Restrict URL Access
A9: Insufficient Transport Layer Protection
A10: Unvalidated Redirects and Forwards

Your organization has determined that the **UltraCompare** application has a **High** business criticality. For most customers, applications with a Medium or higher business criticality indicate applications that are mission critical for the organization. As such, for the **UltraCompare** application, Veracode conducted the following automated security assessments, employing the techniques outlined above:

Analysis Type: Static
Analysis Date: April 17, 2018
Scan Name: 13 Apr 2018 Static 3rd iteration

Summary of the final findings, after mitigations:

Flaw Severity	Flaw Count
Very High	0

Note of Qualification:

- This degree of assurance provided by any assessment is contingent on: (*i*) the integrity of information provided by the organization during the assessment process; (*ii*) the organization's willingness to allocate the resources necessary to execute a level and scope of assessment appropriate to the security characteristics of the application and the sensitivity of information assets in the environment, (*iii*) the organization's execution of recommended remediation measures.
- No methodology definitively proves the absence of vulnerabilities.
- Following assessment and remediation, modifications to an application, its platform, network environment, and new threat vectors may result in new application security vulnerabilities.

Sincerely,

Ellen Nussbaum
Senior Vice President, Services
Veracode, Inc.
enussbaum@veracode.com