ACCUVANT LABS

Euclid Express Application Testing

Euclid / Project Number: OP-106721

Revision Number: 1.0

Date: 10/8/2014

Introduction

Internet facing applications can potentially have multiple vulnerabilities that would allow a malicious party access to private information. The risk associated with these applications is compounded due to the fact that traditional perimeter security mechanisms have no way of protecting against common web application attacks. Web application vulnerabilities generally take advantage of functionality within the application itself rather than the incorrect configuration of a host or missing patch. Defending the enterprise against security threats with today's complex information infrastructure requires a layered security strategy. The strategies in place should be structured to mitigate risk at defined points within the organization. Accuvant works with organizations to locate where effective security measures can be applied, provides a working knowledge of the best in class products and helps implement the final solution into the environment.

Background

Risk reduction through vulnerability assessments is one area where Accuvant helps our customers better their overall security posture. As part of Euclid's ongoing commitment to ensuring the security and integrity of their web based applications and their customer's data, Euclid engaged Accuvant to perform a web application security assessment of the Euclid Express application. The assessment activities were completed in October 2014. Accuvant's approach to security assessments is to attempt to locate application, network and host vulnerabilities, document the findings, create a remediation plan to secure the system, and ensure the remediation efforts taken are successful. There is no guarantee that all vulnerabilities will be located or eliminated.

Scope and Methodology

Accuvant security assessors follow a detailed methodology to uncover system and application vulnerabilities. The assessment encompasses a detailed review of the application interface and data flow, and the servers that support the application. Whenever possible, these efforts occur from both an internal (inside of the network) and external (Internet-based) perspective so that a full picture of the application environment can be obtained without any interference from perimeter security mechanisms. In the case of Euclid Express, the assessment was performed with the following levels of access:

- Standard user access
- Administrative user access

Accuvant consultants utilize multiple commercial and open source security tools, custom scripts, and manual validation techniques to scan for, enumerate, uncover, and exploit vulnerabilities within custom web applications. Commercial scanning tools used such as Burp Suite Pro and Acunetix quickly identify host and application specific vulnerabilities in custom applications, whereas manual techniques such as testing for the ability to manipulate hidden form fields, to inject SQL command strings, to inject JavaScript command strings (cross-site scripting), or to bypass validation routines modifying client-side code, have the ability to find issues in applications not easily uncovered by the automated tools used.

Conclusions

At the end of testing Accuvant observed no critical or high risk vulnerabilities that would allow for direct compromise of Euclid systems or data. Overall, the Euclid Express can be classified as being at a low level of exposure and is well aligned with best practices. Based on the review performed by Accuvant, the application meets the security practices seen by Accuvant within the industry. Euclid's customers can be

assured that Euclid performed proper due-diligence utilizing a trusted third party to independently evaluate the Euclid Express application from an information security standpoint. Based on the findings observed and the remediation steps taken by Euclid, the Euclid Express application follows a best-practices approach for deploying secure web-based applications.

Accuvant LABS sincerely appreciates the opportunity to have served Euclid on this important project and we stand ready to discuss these findings at any time.

About Accuvant

Accuvant is the only research-driven information security partner delivering alignment between IT security and business objectives, clarity to complex security challenges, and confidence in complex security decisions.

Based on our clients' unique requirements, Accuvant assesses, architects and implements the policies, procedures and technologies that most efficiently and effectively protect valuable data assets.

Since 2002, more than 4,500 organizations, including half of the Fortune 100 and 800 federal, state and local entities, have trusted Accuvant with their security challenges. Headquartered in Denver, Accuvant has offices across the United States and Canada. For more information, please visit www.accuvant.com, follow us on Twitter: @Accuvant, or keep in touch via Facebook: http://tiny.cc/facebook553.

1125 17th Street Suite 1700, Denver, CO 80202 | 800.574.0896 | www.accuvant.com