Euclid Express Privacy Validation

Euclid / Project Number: OP-106721

Revision Number: 1.0

Date: 08/12/2014

Introduction

Internet facing applications can contain operational and business logic features that allow disclosure of information to external and internal parties. Some of these features may be implemented by design, and some unintentionally. Euclid has published a privacy policy for their Euclid Express application in order to set user expectations and explain privacy management tools at the user's disposal. Accuvant is working in cooperation with Euclid to review this application, in order to ensure that the application is functioning as described and in compliance with that policy.

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 Human Resources Services Portal application.

While the security assessment activities are ongoing, the initial phase of that assessment included a review of the Euclid Express application's compliance with Euclid's published privacy policy. This privacy policy review and validation was completed in August 2014. Accuvant's approach to this policy validation is to attempt to locate signs of noncompliance in application, network and host behavior, document the findings, create a remediation plan to resolve any issues, and ensure the remediation efforts taken are successful.

There is no guarantee that all instances of noncompliance will be located or eliminated. Workflows, business processes, applications, and data storage systems unrelated to the Euclid Express application are outside the scope of this review.

Scope and Methodology

Accuvant security assessors follow a detailed methodology to uncover instances of noncompliance in system and application behavior. The assessment encompasses a detailed review of the application interface and data flow, as well as 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:

- Unauthenticated user access to development and production instances from the Internet.
- Authenticated, unprivileged user access to standard features of the application from the Internet.
- Authenticated, privileged user access to administrative features of the application from the Internet.

Accuvant's approach to this validation was to reduce the policy to a series of testable hypotheses, then review the application through a combination of manual testing, automated tools, and source code review to find evidence of noncompliance. The specific hypotheses tested are as follows:

- Data is securely deleted on user opt out and is not recoverable.
- When a user opts out of data collection, no further data on that user is collected.
- MAC addresses are anonymized and cannot be recovered on the server side.

- Data is stored securely.
- Data is only shared with Euclid clients.

Conclusions

At the conclusion of testing, Accuvant LABS security consultants observed that the Euclid application was in compliance with the published privacy policy. For each of the hypotheses tested, no instance of application behavior, workflow, or functionality was found to be in contradiction.

Accuvant LABS finds the state of Euclid Express to be consistent with the privacy policy, and Euclid's customers can be assured that they performed proper due diligence utilizing a trusted third party to independently evaluate their systems from a policy compliance standpoint. Accuvant LABS sincerely appreciates the opportunity to have served on this important project and we stand ready to discuss the assessment at any time.

ACCUVANT LABS

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