Seattle Office of Inspector General

May 8, 2020

Police Case Management System Vulnerability

After being notified by the Seattle Information Technology Department (ITD) of a file integrity issue, Office of Inspector General (OIG) auditors identified a security vulnerability in the IAPro case management system, which is used for sensitive investigations conducted by the Seattle Police Department (SPD) and the Office of Police Accountability (OPA). This vulnerability posed a risk to the confidentiality and integrity of materials relating to investigations of force and officer misconduct, as well as investigations conducted by SPD Human Resources. OIG worked with ITD and other stakeholders to deploy a potentially permanent fix to the vulnerability.

Highlights

- OIG auditors, who were authorized users of the system, tested and confirmed a security vulnerability affecting the confidentiality, integrity, or availability of stored investigation files. This was done outside of normal use of the IAPro application, meaning that it was not recorded in the IAPro audit log.
- The impact of this security vulnerability is that any authorized IAPro user could have potentially accessed, modified, downloaded, or deleted sensitive materials with no record of the activity in the IAPro audit log. Similarly, anyone with access to the SPD shared network drive could have potentially accessed or downloaded materials.
- ITD worked with the IAPro developer, CI Technologies, Inc to fix the design issue, update, and distribute the IAPro application to all authorized Seattle users.

Reasons for Review

OIG began a review after IAPro files were inadvertently deleted by an OIG employee. SPD, OPA, and OIG began encountering errors while using the IAPro application and alerted ITD. ITD notified OIG that files had been deleted by an OIG user account, and that they had recovered the files. ITD notified OIG that after the deletion, they put in place an auditing tool to detect future deletion activity outside of the IAPro application. To avoid future incidents and safeguard the integrity of IAPro files, OIG began researching how the file deletion was possible and if any other potential security concerns existed within the IAPro application.

Causes of Security Vulnerability

During the review, OIG auditors found a security vulnerability in the design of the application and a specific type of remote file storage used by Seattle since the installation of the software in 2014. The parent company of IAPro, CI Technologies, Inc., confirmed the security vulnerability and acknowledged that other customers had experienced similar issues.

OIG Tested and Confirmed Security Vulnerability

Using the security vulnerability, OIG auditors were able to view and open SPD and OPA investigation files related to investigation and review of use of force. OIG was also able to access SPD Human Resources files but deliberately did not open these files out of an abundance of caution.[1] This access was not through normal use of the IAPro application, meaning that it was not recorded in the IAPro audit log.

OIG auditors created a test case in the IAPro application with a sample Word document. Using the security vulnerability, auditors were able to access the document and modify it. The IAPro audit log showed no record of the file being accessed or modified.

Security Vulnerability Allowed Unauthorized Access of IAPro Files

IAPro generates an internal audit trail of user activity within the application. This includes records of access to investigation files, including actions such as adding, modifying, or deleting files. However, OIG confirmed that the security vulnerability enabled authorized IAPro users to access, modify, download, or delete sensitive materials with no record of the activity in the IAPro audit log. Further, anyone with access to the SPD shared network drive but without an IAPro account would have been able to access or download materials. However, they would have had no ability to modify the data residing in the IAPro application.

OIG was unable to verify whether any material in IAPro had been compromised. Use of the vulnerability is difficult to trace, requiring timely, manual review of each file suspected of having been accessed, altered, or downloaded. Because records are perishable and may not be accessible after a certain length of time has passed, an analysis of the application's

[1] OIG accesses SPD and OPA investigation files through the course of its routine duties, and thus deemed the risk of opening these files using the security vulnerability to be low. However, OIG does not review SPD Human Resources files as part of its routine work, and so did not open these files using the vulnerability.

data since its inception is not possible. ITD reported that they did not have any indication of past file deletions outside of the IAPro application.

ITD Implemented a Potentially Permanent Fix to Resolve the Security Vulnerability

The presence of the security vulnerability and difficulty in detecting its use posed a severe risk to the integrity and confidentiality of information in IAPro. OIG shared the results of this review with the affected parties, identified several potential options to mitigate the vulnerability, and suggested that SPD and OPA address these issues in consultation with ITD.

As a result, ITD took immediate action to coordinate with CI Technologies to put in place a potentially permanent fix to resolve the security vulnerability. ITD ultimately explored and implemented a different option than those identified by OIG. OIG will provide technical assistance and input as an IAPro user to SPD, OPA, and ITD to continue enhancing the security of IAPro.

Acknowledgements

Without shared commitment to accountability and transparency, OIG would have had difficulty completing its review in a timely manner. OIG would like to acknowledge and thank ITD, SPD, and OPA for their readiness to share information about their processes, and for their collaborative, solutions-focused approach. We consider this an example of the effectiveness of the accountability system when all partners work together to identify and resolve system issues.