Lab #1

By

Patrick Foulis

October 22, 2024

CYB 115 Cybersecurity Fundamentals

Assumption College
Cybersecurity Program

Over the weekend, MassHealth discovered an adverse event that had escalated to the level of an incident. At the end of the workday on Friday, October 18, 2024, update 138.95.3 was pushed to MassHealth's mobile app to solve some minor vulnerabilities within the application's API. However, this release contained a vulnerability that was found and exploited over the weekend. A new patch to the mobile application created a vulnerability that allowed an SQL injection onto the login page where an unauthorized user used spyware to collect usernames. Thankfully, our password encryption enabled those to stay protected, and there have not been any account breaches since the adverse event was discovered. An unauthorized user found this vulnerability and exploited it. The Incident Response team labeled the username harvesting as having an impact of 5/10 because those alone can not reveal the PII that our databases contain, but it most definitely weakens its protection. The mobile application was listed as an impact of 2/10 because it only contains limited information, is very early in our defense-in-depth structure, and is easily patched. The unauthorized user was labeled as an impact of 1/10 since they have minimal knowledge of our internal system workings, and no action needs to be taken within the corporation. The breach weakens the confidentiality of our user's healthcare and personal information.

To remediate the breach, the Information Security Team must complete certain tasks in response to the incident. The vulnerability within MassHealth's mobile application needs to be patched, and the security of users' accounts needs to be re-established. There needs to be an update to our monitoring system for the foreseeable future to detect if this breach escalates any further and if other information assets within the company are compromised in the future. Our change management process must be reviewed to ensure that a scenario like this does not happen again. Finally, we must inform the public and users about the breach in compliance with our human resources department.

To complete these tasks, the Incident Response team needs to direct other teams within the Information Security Department to take certain actions. First, the mobile app needs to be reverted to the version that did not contain the SQL injection vulnerability. After that, the team that pushed out the faulty patch needs to fix the existing vulnerability so that both the SQL injection and API vulnerabilities can be fixed. To address the compromised security of users' accounts, the team needs to force users to reset their username and passwords and inform them within the notification that the old username may have been breached. A separate project team has been created to implement multifactor authentication to further secure their accounts. Incident Response team members will document the incident and direct analysts to update the monitoring system in case the breach is larger than expected. Members of the change management team will review and revise their policy and testing procedures so another form of this breach does not repeat itself. The Incident Response Plan will also be referenced to explain how to notify the public of the breach.

These actions will result in the addition of outsourced penetration testing before the release of major updates to the mobile application. The change management process will be added, along with extra security reviews, before any update is pushed. Any other actions that HIPPA requires will be followed to ensure that all security guidelines for medical information are followed. The scope of the breach will be closed to only usernames, and thankfully, no personally identifiable information will have been lost within the breach.

Certification of Authorship

Submitted to Instructor: Professor Snow

Student's Name: Patrick Foulis

Date of Submission: October 22 2024

Purpose Submission: In fulfillment of course requirement(s) in CYB 115 Cybersecurity Fundamentals

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this purpose.

Name: Patrick Foulis