**Module Five Case Study**

Joseph Veneski

Department of Computer Science, Southern New Hampshire University

CS-405 Secure Coding

Professor Kaan Esendemir

April 7, 2024

**Module Five Case Study**

**Introduction:**

In June of 2023, Progress Software’s MOVEit Transfer services which contained a zero-day vulnerability was exploited by Lace Tempest or Cl0p a group of ransomware hackers (Kost, 2023). The exploit, CVE-2023-35708, allows for potential SQL injection attacks allowing unauthorized access to database content (National Institute of Standards and Technology, 2023). According to UpGuard, the breach impacted 94 million users, over 2500 organizations of which the majority were US-based, and over $15 billion in damages (2024). Notable impacted organizations include the US Department of Energy, Johns Hopkins University, First National Bank and others making this a very high-profile breach.

<https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability>

**Description:**

The security vulnerability exploited by hacker groups led to exposure of personal identifiable information and financial information of users from numerous high-profile organizations including Shell PLC, British Airways and more. According to a class action lawsuit over the data breach plaintiffs allege, “Progress failed to implement adequate security measures, monitor its network, properly train its employees, or provide timely notice of the incident” (Brown, 2023). Some potential users impacted by the breach were not notified by Progress, but rather customers who used Progress Software’s MOVEit file transfer services.

**Threats:**

The vulnerability if left unpatched allows malicious actors to implement SQL injection attacks which could be used to delete databases and wreak havoc, steal personal and financial information, or learn more about the structure of the targeted database for future attacks. This breach not only increases the risk of users having their identity stolen but also degrades the user trust of the organizations impacted.

**Prevention:**

The recommended mitigation strategy suggested by NIST is to update to the latest patches. In addition, common SQL injection prevention strategies include parameterizing queries, use of stored procedures, and allow-list input validations or heuristic detection methods for potential unsafe input (OWASP, 2024). Additionally, following the principle of least privilege can further reduce the potential for harmful impact by bad actors limiting the amount of access they gain. Security policies such as input validation, mandating use of parameterized queries, and enforcing principle of least privilege will help prevent this type of attack.

**Summary:**

The MOVEit data breach of 2023 which was the result of the exploitation of zero-day vulnerability CVE-2023-35708, highlights the importance of implementing robust security measures to protect sensitive data. The incident led to unauthorized access and potential exposure of up to 94 million users across over 2500 organizations including Johns Hopkins, the U.S. Department of Energy and many others. The breach resulted in significant financial damage estimated at about $15 billion in addition to the trust damage of affected organizations.

Authentication measures are one of the first steps in a layered security approach and should include robust measures such as multi-factor authentication. Verification of users through multiple mechanisms can significantly reduce the risk of unauthorized access.

Authorization of properly authenticated accounts is another layer to tighten security. Users should only be given access to the resources required to complete their tasks following the principle of least privilege. Limiting the access of accounts to only what is necessary can further reduce the amount of harm bad actors can inflict and protect highly sensitive data.

Accounting of all activity is an essential part of security as well as being a requirement for many regulations. Monitoring and logging of events can increase response time by identifying unusual activity or modifications to data. If authentication and authorization fail, accounting is another layer to bolster defense and catch bad actors.

The principle of Defense in Depth involves utilizing a layered security approach to protect data and resources. If one layer of security is penetrated, there are still more defenses that attackers must get through. In the context of the MOVEit breach, maintaining the most up-to-date patches for software, encrypting data at rest and in transit, and regular vulnerability and activity monitoring could create a layered defense in depth approach to mitigate risks. This case illustrates the consequences of neglecting a comprehensive, layered approach to security, underscoring the imperative for organizations to continuously evolve their security practices in response to emerging threats and vulnerabilities.

**References**

Brown, C. (2023). *Progress Software Hit With Class Action Over MOVEit Data Breach*. Bloomberg Law. <https://news.bloomberglaw.com/privacy-and-data-security/progress-software-hit-with-class-action-over-moveit-data-breach>

Chin, K. (2024). *Biggest Data Breaches in US History*. UpGuard. <https://www.upguard.com/blog/biggest-data-breaches-us>

Kost, E. (2023). *The MOVEit Zero-Day Vulnerability: How to Respond*. UpGuard. <https://www.upguard.com/blog/the-moveit-0-day>

National Institute of Standards and Technology. (2023). *CVE-2023-35708 Detail*. National Vulnerability Database. <https://nvd.nist.gov/vuln/detail/CVE-2023-35708>

OWASP. (2023). *SQL Injection Prevention Cheat Sheet*. <https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html>

Progress. (2023). *MOVEit Transfer and MOVEit Cloud Vulnerability.* <https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability>