Vulnerability Assessment Report

20 December 2023

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 2023 to August 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

Conducting a vulnerability analysis on our open-access database server is imperative to safeguard the core interests of our e-commerce company. The database server, being a repository for valuable customer information, serves as a vital asset to our business operations. The unrestricted access to this server poses a significant risk, as it compromises the confidentiality and integrity of sensitive data. Securing the server is paramount to prevent unauthorized access, potential data breaches, and the associated legal and reputational repercussions. A disruption or disablement of the server could have severe consequences on our ability to serve customers, potentially leading to financial losses and damage to our brand reputation. Thus, this analysis is essential for identifying and mitigating vulnerabilities to ensure the resilience and sustainability of our business operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Disrupt mission-critical operations*	*2*	*3*	*6*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

Approach

The risks evaluated in this vulnerability assessment were scrutinized with a focus on the data storage and management procedures of our business. Potential threat sources and events were identified based on the likelihood of a security incident, taking into account the open access permissions of the information system. The severity of potential incidents was assessed by weighing them against the impact on day-to-day operational needs. This approach ensures a comprehensive analysis that considers both the intrinsic vulnerabilities in our data handling practices and the potential consequences of security incidents arising from the open accessibility of our database server.

Remediation Strategy

To effectively address the identified risks, specific security controls are recommended:

Principle of Least Privilege (PoLP):

Current Controls: Review and strengthen existing access controls.
Recommendation: Implement a comprehensive access review, introducing Role-Based Access Controls (RBAC) to restrict permissions based on job responsibilities.

Impact: This approach minimizes the risk of unauthorized access, ensuring users have only essential access, aligning with the open accessibility vulnerability.

Defense in Depth:

Current Controls: Evaluate and enhance existing defense mechanisms.
Recommendation: Implement network segmentation, deploy Intrusion Detection and Prevention Systems (IDPS), conduct regular security audits, and establish continuous monitoring capabilities.
Impact: A multi-layered defense strategy fortifies the system against diverse attack vectors, addressing the risks associated with the open accessibility of the database server.

Multi-Factor Authentication (MFA):

Current Controls: Assess and strengthen existing authentication methods.
Recommendation: Enforce MFA for system access, requiring users to provide multiple forms of identification.
Impact: Adding an extra layer of user identification mitigates the risk of unauthorized access, especially in scenarios where credentials may be compromised.

Authentication, Authorization, Accounting (AAA) Framework:

Current Controls: Evaluate and enhance the current AAA framework.
Recommendation: Strengthen authentication processes, define and enforce authorization policies, and maintain comprehensive accounting logs for auditing.
Impact: This comprehensive approach tightens control over user access, reducing the risk of unauthorized activities and aligning with potential threats identified in the assessment.
These security controls provide targeted and realistic measures to remediate or mitigate the identified risks, ensuring a more secure information system aligned with the unique vulnerabilities identified in the vulnerability assessment.