Vulnerability Assessment Report

1st January 2024

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 2024 to August 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

Our database server is a key asset to the business that stores customer, sales, and other customer related data that is used for import data analysis tasks needed to optimize business performance and make future planning decisions. Loss of this server would greatly hamper our business because we would no longer be able to perform business analytics tasks, making our business decisions unreliable, and preventing us from making informed marketing choices based insights from customer and sales data. Therefore, the purpose of this vulnerability assessment is to evaluate how our current system architecture increases the risk from vulnerabilities, and enable us to strengthen security and prevent their exploitation.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee	*Alter/Delete critical information*	*1*	*3*	*3*
Hacker	*Obtain sensitive information via exfiltration.*	*2*	*3*	*6*
Storage	*Disrupt mission-critical operations.*	*2*	*2*	*4*

Approach

The approach we took to conduct this report took into account how the data was currently stored and managed. Therefore, when we evaluated threat sources and threat events, we attempted to determine their likelihood based on the public availability of the server and lack of permissions. The severity was determined based on how the threat event would impact the ability of users to continue using the system.

Remediation Strategy

The main remediation strategy is to implement strong authentication and authorization methods on the server. Rather than the information being left publicly accessible, we would implement passwords and other mechanisms to control who is able to access the server. Furthermore, a user-role based mechanism would make it possible to limit user access based on their needs. This would reduce the amount of damage employees could do either intentionally or unintentionally by editing or deleting records. It also makes it more difficult for hackers to initially gain access to user accounts and will help limit the damage they can inflict. We could also consider encrypting sensitive data and using secure connections when transferring data between the user and server.