Vulnerability Assessment Report

1st January 2025

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 2025 to August 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

- *The database server stores all critical business data that supports daily operations, such as customer information, financial records, inventory, and transaction history. Without it, the business cannot function efficiently.*

- *If the data is leaked, stolen, or altered without authorization, it can cause severe damage to the company's reputation and financial stability. For example, if customer data is exposed, attackers might sell it for profit, leading to identity theft, legal consequences, and loss of customer trust.*

- *If the database server becomes unavailable, business continuity will be disrupted. Employees won't be able to access critical data, which may halt operations. This could force the organization to revert to manual processes, making tasks slower, error-prone, and potentially leading to revenue loss.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Alter/Delete critical information	*alters or deletes data that is critical to day-to-day business operations.*	*1*	*3*	*3*
Disrupt mission-critical operations.	*compromises the integrity of information in such a way that prevents the business from carrying out critical operations.*	*2*	*3*	*6*

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.