# Vulnerability Assessment Report

5th September 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 September 2023 to November 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

## Purpose

The database server plays a crucial role in the business by serving as a repository for vital information and facilitating efficient data management. Securing the data on the server is paramount as it safeguards sensitive information, maintains customer trust, and ensures compliance with data protection regulations. If the server were to be disabled, it could disrupt operations, lead to data loss, and result in financial losses due to downtime and potential data breaches, underscoring the server's vital role in business continuity and success.

## Risk Assessment

| Threat source | Threat event | Likelihood | Severity | Risk |
|---|---|---|---|---|
| *Hacker* | *Disrupt Mission-critical operations.* | *3* | *3* | *9* |
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Customer* | *Alter/Delete critical information* | *1* | *3* | *3* |

## Approach

The selected threat sources/events were chosen based on their relevance to the open access permissions of the database server. The primary focus was on potential security incidents that could arise due to this vulnerability. The approach considered the likelihood of these events occurring, given the unrestricted public access, and assessed their severity in terms of their impact on critical business operations. This methodology aimed to prioritize risks that posed a significant threat to the business's data integrity, operational continuity, and overall security posture.

## 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.