Vulnerability Assessment Report

1st 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 June 2023 to August 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

A database server is valuable to a business as it centralizes data management, enhancing efficiency and ensuring consistent, up-to-date information. Securing data on the server is crucial to protect sensitive information, maintain customer trust, and comply with data protection regulations. If a server were disabled, it could disrupt operations, hinder decision-making, and potentially lead to financial losses and damaged customer relationships. Therefore, the server's functionality and security are vital for business continuity and success.

Risk Assessment

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

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 based on the open access permissions of the server to the public.

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.