Vulnerability Assessment Report

1st June 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

Protecting the database server is essential to safeguard customer data, prevent data breaches, and minimize downtime-related losses. The database server contains sensitive information, including PII, making it a prime target for attacks. Ensuring database server security involves implementing robust measures, following best practices, and regularly monitoring and updating the security infrastructure. This helps mitigate the risks associated with data breaches and downtime, which can have severe financial and reputational consequences for companies.

Risk Assessment

Threat source	**Threat event**	**Likelihood**	**Severity**	**Risk**
competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
customer	Alter/Delete critical information	*2*	*3*	*6*
Hacker	*Conduct denial of service attack*	*3*	*3*	*9*
employee	*Disrupt mission 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.