Vulnerability Assessment Report

1st June 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 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The purpose of the risk assessment is to maintain the necessary infrastructure of the in-house server. The server hosts all of the data bases that are crucial to the operation of the company's software products. Conducting regular vulnerability assessment helps to harden our security posture and prevent any malicious attack to create financial loss to the company. Moreover, If an attack were to happen, the server going down would likely create significant reputational damage as well for the company.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Malicious Software	*Supply chain attack from dependency package used to configure the server*	*1*	*3*	*3*
Business partner	*Inject malicious code*	*2*	*3*	*6*

Approach

Risks considered were focused on the risk of external interactions with the server. First we assessed the

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.

Implementation of automated updates on the server linux configuration can