Vulnerability Assessment Report

15th April 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 2024 to August 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The purpose of this vulnerability assessment is to evaluate the risks associated with maintaining a publicly accessible database server that stores sensitive customer and business data. This database is a critical asset for supporting remote operations and enabling employees to identify and engage with potential customers. However, leaving it exposed to the public internet introduces significant risks to data confidentiality, integrity, and availability. Unauthorized access, data breaches, or service disruptions could severely damage the company's reputation, disrupt business operations, and lead to regulatory or financial consequences. The goal of this analysis is to inform decision-makers of these risks and recommend actionable security measures to mitigate them.

Risk Assessment

Threat source	**Threat event**	**Likelihood**	**Severity**	**Risk**
Insider threat (Employee)	*Disrupt mission-critical operations*	*2*	*3*	*6*
External Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Malicious Software (e.g SQL injection)	*Obtain or delete critical information*	*2*	*2*	*4*

Approach

This section documents the approach used to conduct the vulnerability assessment report:

> *This assessment uses a qualitative approach to evaluate potential threats to the company's publicly accessible database server. The selected threat sources—external hackers, insider threats, and malicious software—represent the most significant risks based on the server's exposure, the company's remote work model, and the critical nature of the data stored. These threats were chosen because they align with common attack vectors identified in NIST SP 800-30 Rev. 1 and have a high potential to compromise the confidentiality, integrity, or availability of business data. Evaluating these risks helps prioritize security improvements that protect both operational continuity and customer trust.*

Remediation Strategy

This section provides specific and actionable recommendations to remediate or mitigate the risks that were assessed:

> *To mitigate the risk of unauthorized access by external hackers, the company should restrict public access to the database and implement multi-factor authentication (MFA) for all remote users. Applying the principle of least privilege will limit employee access to only the data and functions necessary for their roles, reducing the potential impact of insider threats. To prevent malware infections, endpoint protection tools and regular system monitoring should be deployed as part of a defense-in-depth strategy. Additionally, adopting the AAA framework will enhance oversight and help detect anomalous user behavior before it escalates into a breach.*