Vulnerability Assessment Report

15st May 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 February 2025 to April 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server is critical to the company's ability to store and retrieve customer and business data, supporting remote employees who need constant access to customer records. It enables essential operations like customer discovery and data analysis. If the database is compromised or taken offline, it would disrupt business activities and reduce customer trust. Securing the data ensures confidentiality, integrity, and availability, which are essential for protecting the company's reputation and revenue.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Competitors	*Conduct Denial of Service (DoS) attack*	*2*	*3*	*6*
Employee	*Disrupt critical operations*	*1*	*3*	*3*

Approach

Risks were evaluated by analyzing the access control weaknesses of the database system, mainly its open access over the internet. The analysis considered the likelihood and severity of threat events involving both external actors (e.g., hackers, competitors) and internal actors (e.g., employees). This approach helped quantify the level of risk and prioritize mitigation strategies for the organization's operational needs.

Remediation Strategy

To reduce the risks found, the database should be set to private and limited to only authorized users. Implementing role-based access controls can help ensure that each user only has access to the data they need. Encrypting sensitive information adds an extra layer of protection against unauthorized access. Regular security audits can help identify any vulnerabilities early. Updating software and patches promptly will also help prevent potential exploits.