Vulnerability Assessment Report

13th August 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 database server is vital to the organization as it stores and manages essential business data needed for daily operations. Securing this data is critical to protect against unauthorized access, data breaches, and service disruptions. If the server were disabled, it could lead to operational downtime, financial losses, and reputational harm.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Malicious Insider	*Gain unauthorized access to database via weak access controls*	*2*	*3*	*6*
External Attacker	*Exploit misconfigured access permissions to steal data*	*3*	*3*	*9*
Malware/Ransomware	*Infect server and encrypt database, causing downtime*	*2*	*3*	*6*

Approach

The risks were selected based on their relevance to the system's access controls and their potential impact on critical business data. Likelihood scores were derived from historical incident patterns, system exposure, and configuration, while severity scores reflected potential operational, financial, and reputational consequences. The assessment was limited by available documentation, the exclusion of active exploitation testing, and the focus solely on access control threats.

Remediation Strategy

Current security measures such as SSL/TLS encryption and stable network configuration should be supplemented with stronger access control policies, multi-factor authentication, and regular account audits. Implementing role-based access control, timely patching, and continuous monitoring can significantly reduce the likelihood of unauthorized access or data compromise. Applying these controls based on the assessment findings will enhance the system's confidentiality, integrity, and availability, ensuring more robust protection of critical business data.