Vulnerability Assessment Report

4/21/2025

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

This database server plays a critical role in business operations, storing sensitive information such as customer data, transaction records, and internal communications. Ensuring the security of this data is essential to maintain customer trust, comply with data protection regulations, and prevent financial loss. A security breach or prolonged server downtime could severely disrupt operations, damage the organization's reputation, and result in legal penalties or revenue loss. This assessment aims to identify vulnerabilities that could impact the server's reliability and to recommend steps for remediation.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Group (Competitor)	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Outsider (Hacker)	*Conduct Denial of Service (DoS) attacks*	*3*	*2*	*6*

Privileged User	*Alter/Delete critical information*	*2*	*3*	*6*
Standard User	*Obfuscate future attacks*	*3*	*3*	*9*
Outsider (APT)	*Install network sniffers*	*3*	*3*	*9*
Software Failure	*Obtain sensitive information via exfiltration*	*2*	*2*	*4*

Approach

The risks evaluated were selected based on the criticality of the database server to business operations and its exposure to both internal and external threat actors. Likelihood and severity scores were assigned based on prior incident records, expert analysis, and known vulnerabilities in similar environments.

Limitations of the assessment include lack of full access to historical system logs and inability to perform intrusive testing due to business continuity requirements. However, network scans, access reviews, and configuration audits were conducted to ensure comprehensive coverage of potential vulnerabilities.

Remediation Strategy

Current security measures include SSL/TLS encryption, limited remote access, firewall rules, and role-based access control (RBAC). To reduce the evaluated risks, the following additional controls are recommended:

Technical Controls:

- Implement intrusion detection and prevention systems (IDPS).
- Enforce multi-factor authentication (MFA) for all privileged users.
- Schedule regular patch management for both OS and database software.

Operational Controls:

- Conduct periodic security training for all employees.
- Establish a change management process for database updates and configuration changes.

Managerial Controls:

- Develop and enforce an incident response policy.
- Perform regular audits to ensure access control compliance.