Vulnerability Assessment Report

1st January 20XX

System Description

The database server runs on the latest Linux operating system, powered by a high-performance CPU and 128GB of memory. It hosts a MySQL database management system and is configured with a stable IPv4 network connection to interact with other internal servers. Security measures include SSL/TLS encryption for data in transit. The server is currently accessible to the public internet, creating a significant attack surface..

Scope

This vulnerability assessment focuses on the current access control configuration of the database server. The evaluation covers a three-month period, from June 20XX to August 20XX, and follows the NIST SP 800-30 Rev. 1 risk assessment methodology. The scope is limited to the confidentiality, integrity, and availability of the server data, excluding physical security or related infrastructure.

Purpose

The database server stores sensitive customer and business information critical to daily operations. As it is accessible to the public internet, the risk of unauthorized access, data exfiltration, or service disruption is significant. If the server were compromised or disabled, it could result in operational downtime, data breaches, and reputational damage, directly impacting revenue and customer trust. This assessment aims to identify and prioritize risks so the business can implement appropriate security measures.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Cybercriminal	*Data exfiltration of sensitive customer data*	*3*	*3*	*9*
Malicious insider	*Unauthorized modification of database records*	*2*	*3*	*6*
Competitor	*Denial of Service (DoS) attack to disrupt ops*	*2*	*2*	*4*

Approach

Risks were evaluated using the NIST SP 800-30 Rev. 1 qualitative methodology. The identified threats were selected based on their relevance to the current system exposure and the potential for significant business impact. The likelihood ratings were determined by considering both historical attack patterns and the attractiveness of the target to malicious actors. Severity ratings were based on the possible disruption to operations, legal implications, and reputational harm.

Remediation Strategy

Enhance Monitoring: Deploy intrusion detection systems (IDS) and enable detailed logging for all database queries.

Encrypt Data: Upgrade to modern TLS encryption for all in-transit data and ensure encryption-at-rest for sensitive records.

Improve Network Security: Apply IP allow-listing to limit server access to approved corporate networks.