Vulnerability Assessment Report

24th June 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 database server is valuable to the business because employees often refer to / query the database to find information that will introduce customers directly to the business.

It is important for a business to secure the data on the server so that the information contained in the server cannot be accessed by those who are not intended to use it. That information could include both employee and customer's PII (Personally-Identifiable-Information) such as name, email address, social security number and IP addresses as well as SPII (Sensitive Personally-Identifiable-Information) which is PII that if lost, stolen, or disclosed without authorization could cause significant harm to an individual directly or even the business itself.

If the server was disabled by a threat, the impact to the business could be catastrophic. Sensitive information would be vulnerable to exploit, and business that relied on the server to function would come to a halt. This could include but is not limited to; customer base inquiry, financial transaction data, PII and SPII depending on the source of the threat. Threat sources can range from human to technological to environmental sources such as insider groups or vendors, hackers, malicious code/ corrupted database files, failures of equipment and hardware due to resource depletion or even operating conditions.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*2*	*3*	*6*
Outside User /Hacker	*Conduct Denial of Service (DoS) attacks.*	*2*	*3*	*6*
Standard User/ Group User (Employees, customers, Business partners, or Suppliers)	*Alter/Delete critical information*	*3*	*3*	*9*

Approach

The rationale behind the risks described above is that they are the most likely and have the highest level of severity for each likelihood for this case.
For each threat, qualitative values of 1 through 3 are given as a likelihood score based on the intent, capabilities and potential, and then qualitative values of 1 through 3 are given as a severity score defining the impact and effects each threat pose to business operations and assets. For likelihood, a score of 2 means the threat source is somewhat likely to initiate, and could significantly reduce the functionality of organizational operations, and 3 meaning the threat source is almost certain to initiate a security event, which could have multiple, severe, and/or catastrophic effects on operations and assets. Severity scores at 3 define threat sources as almost certain to initiate security events, which could also have multiple, severe, or catastrophic effects on business operations and assets.
Limitations of the assessment are that this is a qualitative assessment of one remote server defining threat sources and events of the highest likelihood and severity instead of a comprehensive assessment for all known assets and possibilities for the quarter of June 2024 to August 2024.

Remediation Strategy

The current technical, operational and managerial controls currently implemented to secure the system include updated to most recent version of the operating system, a MySQL database management system, and SSL/TLS encrypted connections. First,

technical controls such as implementation of PKI (Public Key Infrastructure) to address the exfiltration of sensitive information, IP Whitelisting to only allow access based on IP address (i.e. all the remote IP addresses of the employees' workstations,) and MFA (Multifactor Authentication) to enforce the use of secure connections by those authorized to access the database. Then configure a firewall rule to enable port filtering to block all unwanted incoming traffic to port 3306 which is dedicated to MySQL connections at the network layer to mitigate the ability for a malicious actor to initiate a DoS attack on the server. Moreover, regular security audits should be performed on the existing MySQL database management system logs to identify any ongoing suspicious behavior. Finally, implement managerial control to establish a comprehensive security awareness program for all employees with database access to ensure they understand the importance of data protection and adhere to best practices for secure operations, so that critical data is never mistakenly altered or deleted. Each of these recommendations strengthens the security posture by addressing different layers, technical, operational, and managerial, ensuring the organization's system operates securely and is resilient against potential threats.