Vulnerability Assessment Report

1st January 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 an extremely valuable asset for the business, and should be treated as one of the top priorities in terms of security. It is important for the business to secure the data on the server because it contains highly sensitive information that could potentially be misused/destroyed by a malicious actor. If the server is disabled or malfunctions due to a malicious actor, its impact on the business would be severe. Not only would important files and data potentially be lost, but the business would suffer a reputation loss as well. It is highly important to keep the server safe and strong enough to withstand attacks.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Obtain sensitive information via exfiltration	1	3	3
Hacker	Perform reconnaissance/surveillance	2	2	4
Malicious software	Disrupt mission critical operations	2	3	6

Approach

The three most likely threat sources in this scenario would be competitors, hackers, or simply malicious software uploaded accidentally/on purpose. Since the database is open to the public, competitors would easily be able to see critical data that might give them leverage. Hackers can also easily perform reconnaissance scans of the company's data. Lastly, due to the nature of being public, anyone with the technical skills could potentially upload a malicious software or application onto the server, and disrupt mission critical operations.

Remediation Strategy

The business should implement authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Furthermore, encryption of data in motion should use TLS instead of SSL.

The company can also implement IP whitelisting, which will block any unallowed traffic from entering the network. The company must be cautious about which IP's are being blocked, and also should keep in mind scalability concerns.