Vulnerability Assessment Report

1st September 2023

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 2023 to August 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database is of key importance to the organization's business operations. Most of the employees in the organization work remotely and hence need frequent access to the database to carry out business activities. The data stored on the database is crucial for business and thus any disruptions to the operations of the server on which the database is hosted can cause a serious impact on the organization's business. The impact may range from financial loss to user data being breached therefore securing the server is of utmost importance to ensure streamlined flow of business operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Privileged user	*Alter/Delete critical information.*	*2*	*2*	*4*
Outsiders	*Conduct Denial of Service (DoS) attacks. Disrupt business critical operations.*	*3*	*3*	*9*
Malicious software	*Install persistent and targeted network sniffers on organizational information*	*3*	*2*	*6*

	systems.			

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

Privileged users such as a system administrator unintentionally or deliberately pose a threat to the server due to their elevated rights and access to the server. Since the database server is open to the public it is very likely that outside threat actors will target it and can cause great damage to critical business operations. Outside attackers may install malicious software which may passively or actively pose a threat to the organization's information systems.

Remediation Strategy

Implementation of 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. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.

Implementing least privilege policy will help in reducing the likelihood of accidental damage to the database server. Only the users who require access to database server's critical operation configurations may be allowed to do so.

Implementing firewalls and intrusion detection systems will allow detecting malicious traffic trying to harm the database server and implementing robust authentication and authorization mechanisms will ensure no unauthorized entity can access the database server.

Installing and configuring security softwares such as antivirus and network traffic monitoring software will ensure that no malicious software is actively or passively posing a threat to the information systems. Updating and patching these softwares on a regular basis will help to detect the latest threats.