Vulnerability Assessment Report

19th October 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

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
  The company stores information remotely using the server, which is crucial for business operations as many of the company's employees work remotely around the world.
- *Why is it important for the business to secure the data on the server?*
  It's important for the business to secure the data as it contains information about potential customers. It's important to secure this information so threat actors cannot use it for their bad intentions.
- *How might the server impact the business if it were disabled?*
  The business would suffer in generating revenue, and its reputation may be negatively impacted, which could further damage the business in the future.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee	Disrupt mission-critical operations.	2	3	6
Customer	Alter/Delete critical information	1	3	3

Hacker	Obtain sensitive information via exfiltration	3	3	9

Approach

The risks that were considered include 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.

Remediation Strategy

The implementation of the AAA framework of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes enforcing strong password policies, role-based access controls, and multi-factor authentication to limit user privileges. Furthermore, the encryption of data in motion should be facilitated using TLS instead of SSL.