Vulnerability Assessment Report

1st November 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 intended outcome of this assessment is to communicate the risks posed by the remote database server, as it currently exists. This server is valuable to the business as storage for customer information and analytical data. It is important to secure this asset so that its integrity remains intact. Were this server be disabled, the business would lose access to potential customers that could result in lost business.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker	Conduct Denial of Service (DoS) attacks	*3*	*3*	*9*
Employee	Alter/Delete critical information	*3*	*2*	*6*

Approach

The risks associated with an open server were focused on. Threats revolving around business disruption due to malicious intent from external and internal parties were considered. The likelihood of these events was graded based on ease of committing and opportunities available. The severity was graded based on the potential impacts to business operations.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms, including the principle of least privilege, are critical. The server should not be open to the public. Only internal personnel should have access and within that, there should be varying levels of privileges based on work. Furthermore, MFA should be in place to improve authentication of the user requesting data. Encryption of data using TSL instead of SSL should be used to prevent misuse of sensitive information that is business critical.