Vulnerability Assessment Report

1st January 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 covers a period of three months, from June 2022 to August 2022. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The remote database server is an extremely valuable asset to the company that stores all its information. Many of the employees work remotely from locations all around the world, and regularly query data from the server to find potential customers.

Securing data on the server is crucial, and doing so will reduce the attack surface area and prevent a security breach. Failure to secure the server will impact business continuity, and potentially cause leaks of information that can severely damage the company's reputation and finances.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Advanced Persistent Threat (APT)	*Obtain sensitive information via exfiltration.*	*3*	*3*	*9*
Malicious Software	*Deployment of malware into the internal network.*	*2*	*3*	*6*
System Administrator	*Stealing information, damaging equipment, leaking company data and intellectual property.*	*1*	*3*	*3*

Approach

The risks being measured considered the data storage and management procedures of the business. Potential threat sources and events were determined using the likelihood of a security incident due to the open access permissions of the database. The severity of potential incidents were weighed against the impact on daily operational needs.

Remediation Strategy

Implement a defense-in-depth strategy, public key infrastructure, and least privilege controls to mitigate risk. This includes configuration of stateful firewalls, role-based access controls, multi-factor authentication, and asymmetric encryption. Data in transit should be encrypted using TLS instead of SSL. Additionally, IP allow-listing to corporate offices will prevent random users from connecting to the database.