Vulnerability Assessment Report

29th 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 purpose of this vulnerability assessment is to evaluate the size of the vulnerability, potential risks it may be exposing the company to, and find proactive solutions to these vulnerabilities. Having the database open to the public creates a severe vulnerability, since this is critical information all employees around the world depend on to perform their routine tasks. It also contains sensitive information, like PII of potential customers. It is important that the business secures the data on the server to prevent any unauthorized user or threat actor from gaining access to that information and potentially leak, alter, and/or destroy it. This would have grave consequences on the business, as it could lead to a disruption in operations, damage to reputation, and failure to meet compliance and regulations.

Risk Assessment

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

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.

Remediation Strategy

The implementation of authentication, authorization, and auditing measures to guarantee that only authorized users can access the database server. This involves enforcing strong passwords, applying role-based permissions, and using MFA to ensure authorized user access. Data in transit should be encrypted using TLS instead of SSL, and IP allow-listing should be used to restrict database access to corporate office networks only.