Vulnerability Assessment Report

22nd September 2024

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 2024 to August 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server is the heart of our business considering we are an e-commerce company. Many of our employees work fully remote and regularly access the server to do their job. If data on this server is not secure, malicious actors could easily access the database and compromise our customers' data. We would have to shut down the server for an indefinite amount of time until we clear up the threat, which will make it impossible for our employees to do their job.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Obtain sensitive information via exfiltration	*3*	*3*	*3*
Employee	Alter/Delete critical information	*2*	*3*	*6*
Hacktivist	Disrupt mission-critical operations.	*1*	*3*	*9*

Approach

A competitor is a potential threat because they have an incentive to learn as much about our customers to form their own strategies on how they can win them over. This poses a big risk to the long and short term sales of the company. A disgruntled employee has the ability to easily alter/delete information from the database which could set us back any number of months/years. Access controls need to be in place to prevent such a scenario. Also, fully remote employees are more likely to follow through with a plan to damage the company due to having a less personal connection. Hacktivists might try to use the public database to disrupt our business operations if they disagree with some morality behind the products that we sell or how we make them.

Remediation Strategy

Principle of least privileged needs to be implemented asap, with the first priority being to remove public access to the data. Then we can work on determining access privileges among specific employees/departments. On top of this, we should integrate authentication, authorization, and auditing. This we bring tighter control over our employees' access to the database and further prevent the possibility of a hacktivist accessing our database.