Vulnerability Assessment Report

1st January 2025

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

Consider the following questions to help you write:

> *Information retrieved from databases is the cornerstone of the daily operations of an e-commerce company. The data stored in these databases should be confidential due to the security of the customers and their trust in the company. A temporary or total loss of data would have serious financial and reputational consequences.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Malicious software	*Infect server and loss and data*	*2*	*3*	*6*
Hacker	*data encryption and payment request*	*2*	*3*	*6*

Approach

In this assessment, we focused on the potential misuse of data by competitors as well as the loss of data caused by malware infection or data encryption by hackers seeking financial gain.

We believe that the servers are built on solid hardware, which is not prone to failure. Since the database is public, it is very likely that someone will try to exploit this for their own benefit.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.