Vulnerability Assessment Report

12th 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. The database server is open to the public, posing a very serious vulnerability.

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 serves as a centralised store for product and customer data, but is currently publicly accessible. Company employees use this data to identify potential customers for business development. If the server were offline or compromised, it could result in significant monetary losses for the company. Additionally, employees would be unable to perform their work functions during any downtime, and if a competitor gains access to the customer data, they could potentially acquire our clients.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Can get access to sensitive customer data via exfiltration*	*3*	*3*	*9*
Hacktivist	*Disrupt mission-critical operations*	*2*	*3*	*6*
Competitor	*Alter/Delete critical information*	*2*	*3*	*6*

Approach

This assessment follows a qualitative approach based on the analyst's experience and professional judgment. This method was selected because it allows for rapid evaluation of newly identified vulnerabilities and provides stakeholders with an accessible, high-level understanding of business risks without requiring extensive quantitative data collection.

An e-commerce company can be easily targeted by hackers seeking the vast amount of personal information it contains, and by hacktivists for ethical or ideological reasons. Additionally, a publicly accessible database is extremely attractive to competitors who may steal customer data to gain a market advantage or sabotage operations to cause financial losses.

The risk assessment considered current business operations and security standards. We followed NIST SP 800-30 Rev. 1 to identify relevant threat sources and events, and to rank their likelihood and severity. Risk levels were calculated as the product of likelihood and severity (likelihood × severity).

Remediation Strategy

The primary vulnerability arises from the database being publicly accessible without proper access controls. Implementing the principle of least privilege will restrict employee access to only necessary data with read-only permissions where it is appropriate. MFA and the AAA framework should be used to verify user identities and also track database activities. Additionally, deploying an IDS/IPS will monitor for abnormal access patterns and potential threats. These layered security controls will maintain business functionality while significantly reducing risks from external attackers and internal mistakes.