

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 2025 to August 2025. [NIST SP 800-30 Rev. 1](#) is used to guide the risk analysis of the information system.

Purpose

- The database server is critical to business operations because it stores customer information that employees query to identify potential customers and support sales activities. Since the company operates with remote employees worldwide who depend on this data for daily work, securing the server protects both business operations and customer trust. If the server were disabled or compromised, the company would face operational disruptions affecting employee productivity, potential data breaches leading to legal and financial consequences, and damage to the company's reputation that could drive customers to competitors.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	<i>Obtain sensitive information via exfiltration</i>	3	3	9
Advanced Persistent Threat (APT)	<i>Conduct Denial of Service (DoS) attacks</i>	2	3	6
Malicious	<i>Alter/Delete critical information</i>	2	3	6

software				
----------	--	--	--	--

Approach

The three threat sources identified represent the most significant risks to a publicly accessible database server. Hackers targeting the open database represent a high likelihood threat because the server has been publicly accessible for three years, giving attackers ample time to discover and exploit this vulnerability. APT groups pose a moderate but severe risk since e-commerce companies store valuable customer data that nation-states or organized groups might target for financial gain or competitive advantage. Malicious software represents a moderate likelihood because the open database increases the attack surface for malware that could corrupt or destroy critical business data. These threats were prioritized based on their potential to disrupt business operations, compromise customer data, and damage the company's market position.

Remediation Strategy

Close public access to the database server immediately and implement IP allow-listing to restrict connections only from corporate office locations and verified remote employee IP addresses. Deploy multi-factor authentication (MFA) for all database access combined with role-based access controls following the principle of least privilege, ensuring employees can only query data necessary for their specific job functions. Establish an Authentication, Authorization, and Accounting (AAA) framework to monitor all database access attempts and maintain detailed logs of queries performed. Apply defense in depth by adding an intrusion detection system (IDS) to monitor traffic patterns and alert security teams to suspicious activity, while also implementing database activity monitoring to detect unusual query patterns that might indicate data exfiltration attempts.