Vulnerability Assessment Report

December 18, 2025

System Description

The system under assessment is a remote database server used by a small e-commerce business to store customer and business data. Employees access the database remotely to query customer information. The server is publicly accessible over the internet and has been left open since the company's launch, creating a significant security concern.

Scope

This vulnerability assessment focuses on the database server's access controls and exposure to the public internet. The assessment evaluates risks related to unauthorized access, data exposure, and potential business impact. NIST SO 800-30 Rev 1 is used as guidance for identifying and analyzing risks.

Purpose

The purpose of this assessment is to identify security risks associated with the publicly accessible database server and to communicate those risks to decision makers. The report also provides recommendations to reduce risks and improve the organization's security posture.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
External attacker	*Unauthorized access to customer data*	*3*	*3*	*9*
Cybercriminal	*Data breach and data theft*	*3*	*3*	*9*
Malicious actor	*Service disruption and denial of service*	*2*	*2*	*4*

Approach to the organization

This assessment uses a quantitative risk analysis approach guided by NIST SP 800-30 Rev

Threat source, threat events, likelihood, and potential impact were evaluated to determine overall risk to the organization.

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 data in transit using TLS and disable deprecated SSL protocols. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.