Vulnerability Assessment Report

28th December 2023 / Brian Trujillo

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 2023 to August 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The purpose of this vulnerability assessment: Firstly, to evaluate the risk associated with the database server being open to the public, which includes identifying potential vulnerabilities that could be exploited. Secondly, to quantify the impact that such vulnerabilities could have on our e-commerce operations, customer trust, and the company's reputation. Lastly, the assessment aims to provide a set of recommended actions to mitigate identified risks, ultimately guiding the company toward a more secure data management practice. The findings and recommendations will be vital in driving informed decisions by the company's leadership, ensuring that data security is not only understood but also integrated into the operational framework.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hackers	*Exploitation of vulnerabilities which can lead to malware and ransomware to be injected in the*	*4*	*5*	*20*

	system.			
Insiders	*Accidental data leak or intentional data misuse*	*2*	*4*	*8*
Unauthorized External Actors	*Unauthorized data access and theft*	*4*	*5*	*20*

Approach

I focused on those with the potential to significantly impact our e-commerce operations, particularly unauthorized access and data breaches. The likelihood and severity scores for each risk were derived from industry-standard risk matrices, historical incident data, and current cybersecurity trends. The limitations of this assessment were that it was a point-in-time evaluation and could not account for future vulnerabilities introduced by new threats or system updates.

Remediation Strategy

Recommend implementing layered technical controls including firewalls, intrusion detection systems, and regular penetration testing. Additionally, operational controls such as strict access management and regular security training for employees are crucial. Managerial controls should involve establishing a comprehensive security policy and a rapid incident response plan. These controls are chosen for their effectiveness in reducing the identified risks and are aligned with best practices for securing similar e-commerce platforms. The implementation of these recommendations will significantly enhance the overall security posture of the system by not only addressing the identified risks but also by establishing a robust framework for ongoing security management.