Vulnerability Assessment Report

13rd October 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.

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

- A database server is valuable to a business as it centralizes data, enabling easy access to business intelligence from multiple devices.
- The organization in this scenario has multiple remote employees, and their work depends on the database. If it were disabled, employees would not be able to access the information they need to perform their regular work.
- The insecurity of the database can lead to serious issues like non-compliance with regulations, data breaches, and damage to the organization's reputation. Risk Assessment

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Employee	*Alter/Delete critical information*	*2*	*3*	*6*
Hacker	*Conduct Denial of Service (DoS) attacks.*	*3*	*2*	*6*

Approach

Keeping a database server open to the public can expose it to significant security risks, such as unauthorized access, data breaches, and other cyber threats. If the database is disabled, not only could the organization's reputation be damaged, but operational disruptions could also occur.

Remediation Strategy

The implementation of authentication, authorization, and auditing mechanisms ensures 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. A defense-in-depth strategy will mitigate the likelihood of attacks and make the system more robust.