Vulnerability Assessment Report

1st September 2023

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 will be to ensure that the data being stored on the database server is secure. The assessment will take into account a number of variables, including network configuration, access controls, and disaster recovery. If there were a flaw in any one of these variables, it could result in financial and reputational consequences for the business.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacker	*Conduct Denial of Service (DoS) attacks*	*2*	*3*	*6*
Extreme weather events	*Disrupt mission-critical operations*	*2*	*2*	*4*

Approach

Because the database server is open to the public, it could be easy for anyone, most likely from a rival organization, to query it for sensitive information on which it is stored. Also, because the server is in a remote location, rather than the company's intranet, for example, it is vulnerable to a DoS attack. And if the server is in an area that is prone to extreme disaster events, like hurricanes, tornadoes, or earthquakes, important operations could be interrupted unless backup measures are put in place.

Remediation Strategy

After considering the results of this assessment, it is recommended that the organization implements proper input validation and IP whitelisting to prevent unauthorized users from accessing the database. Also, installing a second processor in the server and placing it in a security zone could reduce the likelihood of an DoS attack. In addition, a hot site can be set up in a disaster-free area so that the data can be backed up and stored there in the event of and extreme weather event.