# **Cyber Security Report**

# Vulnerability : Scope, goals, and risk assessment report

Date: March 8, 2024

## Scope and goals of the audit

**Subject**: Discovery of Vulnerability on Website - Microsoft Terminal Service on Port 3389/tcp Open

**Goals:**

1. **Immediate Mitigation :** Take immediate action to close the Microsoft Terminal Service on port 3389/tcp to prevent further unauthorized access to the server.

2. **Security Patching :** Apply security updates and patches to the operating system and associated software to address any known vulnerabilities and strengthen the overall security posture of the server.

3. **Access Control :** Implement strict access control measures to restrict access to sensitive data and systems, ensuring that only authorized personnel can interact with them.

4. **Continuous Monitoring :** Establish a system for continuous monitoring of the website's security, including regular scans and audits to identify and address any new vulnerabilities or security weaknesses promptly.

5. **Training and Awareness :** Conduct training sessions to educate staff members about the importance of cybersecurity practices and raise awareness about potential threats and how to mitigate them effectively.

6. I**ncident Response Plan :** Develop and implement an incident response plan to guide the response to any security incidents or breaches effectively, minimizing their impact and ensuring a swift recovery.

**Introduction :** This report aims to highlight the security vulnerability discovered on our website, involving the opening of the Microsoft Terminal Service (MS-WBT) on port 3389/tcp.

**Description :** The opening of the MS-WBT (Microsoft Terminal Service) on port 3389/tcp has been detected on our website. This vulnerability exposes the website to the risk of being compromised by attackers targeting security weaknesses in the Microsoft Terminal Service.

## Risk assessment

### Risk description

By opening this service, attackers can remotely access the server and manipulate data stored on the website, as well as gain unauthorized access to information systems.

Risk Assessment

**Identification of Vulnerability**: The identified vulnerability pertains to the presence of an open Microsoft Terminal Service (MS-WBT) on port 3389/tcp on the website. This service, when left open and accessible, poses a significant security risk as it could potentially allow unauthorized users to gain remote access to the server hosting the website. This vulnerability exposes the website to various threats, including unauthorized access, data manipulation, and potential compromise of sensitive information stored on the server.

**Assessment of Threats :**

1- Data Manipulation: With unauthorized access, malicious actors could manipulate the data stored on the server. This could include altering website content, injecting malicious scripts, or deleting critical files, leading to integrity breaches and potential loss of trust among users.

2-Compromise of Sensitive Information: The exposure of sensitive information stored on the server poses a significant risk. Attackers could exfiltrate confidential data, such as user credentials, financial records, or proprietary information, leading to breaches of confidentiality and potential legal implications.

3-Denial of Service (DoS): Attackers may attempt to overload the server with malicious traffic or requests, leading to a denial of service for legitimate users. This could disrupt the availability and accessibility of the website, causing financial losses and reputational damage.

4- Credential Theft: If attackers gain unauthorized access to the server, they may attempt to steal user credentials stored within the system. These credentials could be used for further attacks, such as unauthorized access to other systems or accounts, exacerbating the security risks.

Overall, the presence of the open Microsoft Terminal Service exposes the website to a range of threats, including unauthorized access, data manipulation, compromise of sensitive information, denial of service attacks, and credential theft, highlighting the critical need for immediate mitigation measures.

### Recommendations

1- Close the Service: The Microsoft Terminal Service on port 3389/tcp should be closed immediately to prevent unauthorized access to the server.

2-Security Patching: Apply all necessary security updates and patches to the operating system and any service-related software on the server to ensure protection against known vulnerabilities.

3- implement Access Policies: Implement strict access policies and utilize strong encryption techniques to ensure that access to data is restricted to authorized personnel only.

4- Regular Security Audits: Conduct regular security audits to detect and address any new vulnerabilities that may arise in the system

**Conclusion:** The vulnerability in the Microsoft Terminal Service on port 3389/tcp poses a serious threat to the security of the website. Immediate action must be taken to close the vulnerability and enhance the website's security to protect sensitive data and information.