**NETWORK VULNERABILITY ASSESSMENT REPORT**

**USING NESSUS**

**BY**

**TEMITOPE ILORI**

**UNDER THE SUPERVISION OF EXTION INFOTECH**

**June 25th, 2024**

TABLE OF CONTENTS

[**EXECUTIVE SUMMARY** 3](#_Toc170974250)

[**VULNERABILITY SCANNING AND RESULTS** 3](#_Toc170974251)

[**METHODOLOGY** 4](#_Toc170974252)

[**RISK ASSESSMENT** 4](#_Toc170974253)

[**RECOMMENDED MITIGATION STRATEGIES** 6](#_Toc170974254)

# **EXECUTIVE SUMMARY**

The purpose of this report is to present findings on a comprehensive vulnerability assessment conducted on TEECHRISTY companies’ IT infrastructures. It was performed leveraging a vulnerability scanning tool (Nessus) on 25th June, 2024.

Four hosts were identified, found active and scanned. 57 vulnerabilities were discovered where High, Medium and low severity vulnerabilities were found during the scan, five of these will be delved into.

# **VULNERABILITY SCANNING AND RESULTS**

According to the scan report, the following five vulnerabilities were discovered

Buffer overflow: it allows a local malicious user to cause a overrun of data in network manager and can result to system crash, data corruption and Denial of service

Untrusted SSL Server X.509 Certificate: this result shows that the top of the certificate chain sent by the server do not descend from a known public certificate authority or the certificate was signed by an untrusted Certificate authority (CA) and this can make it easy to carry out a man-in-the-middle (MITM) attack

Server Message Block (SMB) vulnerability: a problem in establishing a connection and transferring data related to SMB was discovered.An impact of this vulnerability is a man-in-the-middle attacks against the SMB server.

CVE-2023-47282: an out-of-bounds write that potentially allows an authenticated user to escalate privilege through local access. Impact of this vulnerability are denial of service, unexpected behavior and system crash

CVE-2023-29483 (Dns python): it allows attackers to interfere with DNS name resolution by quickly sending an invalid packet from the expected IP address and source port. Result shows that dns python stub resolver is vulnerable to a potential Denial of service (DoS).

# **METHODOLOGY**

This provides a structured approach to conducting a thorough vulnerability scan to identify and assess the security weaknesses within the network infrastructure using the following steps

* Preparation and planning
* Reconnaissance
* Leveraging and Installation of a primary vulnerability scanning tool (Nessus)
* Conduct of the vulnerability scan
* Review of scan results

# **RISK ASSESSMENT**

This table comprehensively evaluate and prioritize the risks associated with the identified vulnerabilities

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Vulnerabilities/Plugin names | Description | CVSS | Risk rating | Severity | Solutions |
| Lib n d p >= 1.0 Buffer Overflow | A vulnerability was found in lib n d p. This flaw allows a local malicious user to cause a buffer overflow in NetworkManager, triggered by sending a malformed IPv6 router advertisement packet. This issue occurred as lib n d p was not correctly validating the route length information. | 7.4 | Medium | High | Upgrade to the latest version |
| SSL Certificate Cannot Be trusted | The server's X.509 certificate cannot be trusted. | 6.5 | Medium | Medium | Purchase or generate a proper SSL certificate for this service. |
| Server Message Block (SMB) vulnerability | Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. | 5.3 | Medium | Medium | Enforce message signing in the host’s configuration. |
| CVE-2023-47282 | Out-of-bounds write in Intel Media SDK all versions and some Intel oneVPL software before version 23.3.5 may allow an authenticated user to potentially enable escalation of privilege via local access. (CVE-2023-47282) | 4.8 | Medium | Medium | intel has issued a Product Discontinuation notice for Intel Media SDK software and recommends that users of the Intel Media SDK software uninstall it or discontinue use at their earliest convenience. |
| CVE-2023-29483 Dns python < 2.6. 0 r c1 DoS | The version of dns python installed on the remote host is prior to 2.6.0rc1. It is, therefore, affected by a denial of service (DoS) vulnerability. The dns python stub resolver is vulnerable to a potential DoS if a bad-in-some-way response from the right address and port forged by an attacker arrives before a legitimate one on the UDP port dns python is using for that query. In this situation, dns python might switch to querying another resolver or give up entirely, possibly denying service for that resolution. | 5.9 | Medium | Medium | Upgrade to dns python version 2.6.0r c1 or later. |

# **RECOMMENDED MITIGATION STRATEGIES**

I am providing recommendations based on each discovered vulnerability, considering their severity and the Common Vulnerability Scoring System (CVSS) rating and it goes thus:

BUFFER OVERFLOW

* Immediately apply patches to mitigate root causes of the vulnerability
* Ensure validation and sanitization of all input to prevent malicious data from overflowing buffers
* Implement thorough code review and testing to identify and fix buffer overflow vulnerabilities.
* Conduct network segmentation to limit impact of the vulnerability

Untrusted SSL Server X.509 Certificate

* Implementation of a strict validation checks on server certificates for verification of authenticity and integrity
* Application of Trusted certificate authority
* Employ use of HTTPS for encryption of data
* Regular conduct of monitoring for unauthorized certificates

Server Message Block (SMB) vulnerability

* Configuration of firewall for restriction of SMB traffic to an authorized network
* Network segmentation
* Regular security patches
* Efficient monitoring of SMB to detect and reduce impact

CVE-2023-47282

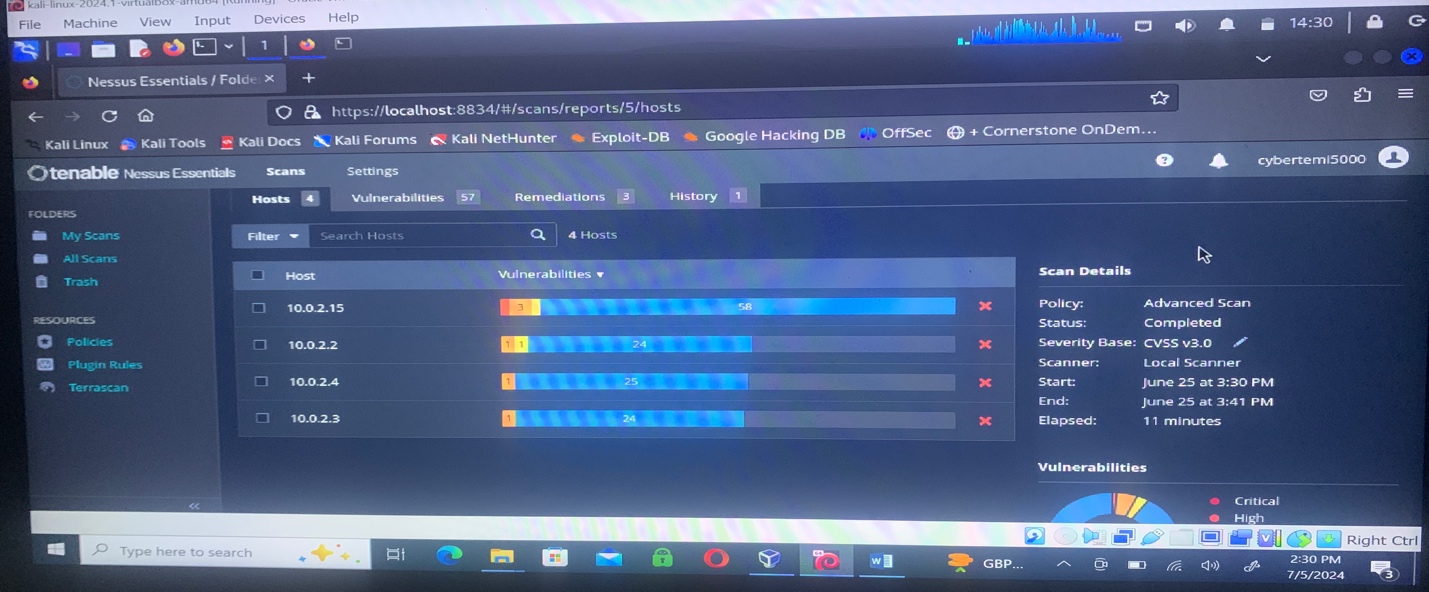
* Update Software
* Apply latest patches provided by Intel
* Restrict user permission
* Use safe functions and apply compiler protections.
* Proper Input validation

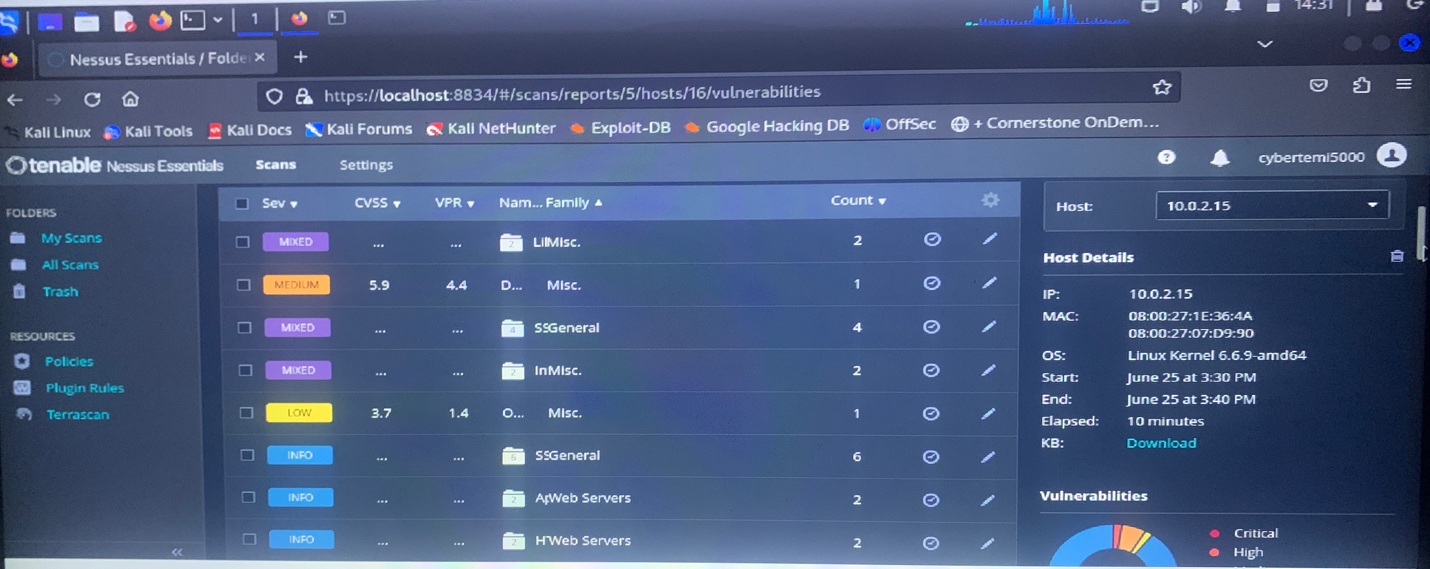
CVE-2023-29483 (Dns python)

* Upgrade dns python and its dependencies to the latest version
* Apply regular security patches
* Regular monitoring of the DNS traffic
* Efficient use of firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to block malicious DNS traffic.

These strategies focus on reducing likelihood and impact of an exploitation. Key strategies that should be implemented are network segmentation, patching and education on the best security practices. Using Nessus as a tool to assess security posture of a network is an effective mitigation strategy aimed to minimize the risk posed by vulnerabilities while maintaining operational efficiency and resilience.

**EVIDENCE OF SCANNED RESULTS**

****

****