Università degli Studi di Salerno
Corso di Penetration Testing and Ethical Hacking

Anno Accademico 2023/2024

Penetration Testing Report
Caso di studio: FormulaX

Cognome Nome	Matricola
Gagliarde Nicolapio	0522501488

Prof. Castiglione Arcangelo

Contents

1 | Executive summary

Il processo di Penetration Testing ha permesso di analizzare le problematiche di sicurezza della macchina FormulaX reperibile sul sito Hack The Box al seguente link:

https://app.hackthebox.com/machines/FormulaX

L'obiettivo è stato quello di analizzare le vulnerabilità che potrebbero colpire gli utenti di FormulaX e vulnerabilità che potrebbero portare all'estrazione di dati riservati e all'accesso completo alla macchina.

Il processo è avvenuto dal giorno 24/05/2024 al giorno 17/06/2024, inoltre l'unica informazione messa a disposizione del Penetration Tester è stata l'indirizzo IP assegnato alla macchina. Quindi si è iniziato dall'analisi dei servizi SSH e HTTP, per poi estendersi alle applicazioni web in esecuzione e alla gestione dei dati e degli utenti sulla macchina FormulaX.

I risultati ottenuti rivelano un **livello di sicurezza basso**, le vulnerabilità più ad alto rischio sono dovute all'assenza di controlli di validazione dell'input ricevuto dagli utenti attraverso i form dell'applicazione web che permette la comunicazione con il chatbot, e all'utilizzo di una versione vulnerabile di Simple-git per la realizzazione dell'applicazione dev-git-auto-update.chatbot.htb. Quindi risulta necessaria l'implementazione di appositi filtri per i dati ricevuti dagli utenti e aggiornare Simple-git a una versione recente. Inoltre bisognerebbe migliorare la gestione e la scelta delle password degli utenti, ed evitare di abilitare agli utenti non admin l'esecuzione di file che richiedebbero permessi elevati.
Se le problematiche di sicurezza rilevate non vengono mitigate, un utente malevolo potrebbe ottenere l'accesso completo al sistema.

Questo report contiene un analisi dettagliata delle vulnerabilità rilevate durante il processo e come mitigarle.

2 | Engagement highlights

L'attività di penetration testing che verrà eseguita ha un fine didattico, pertanto, non è stata fatta nessuna contrattazione con un cliente. Di conseguenza non sono presenti regole di ingaggio, tutta via si riportano i tools utilizzati nelle varie fasi:

- Information Gathering & Target Discovery: è stato usato nmap [10] e p0f [15].
- Enumerate Target & Port Scanning: i tools nmap e unicornscan [12] hanno permesso la scansione delle porte. L'enumerazione è avvenuta usando ssh-audit [14], WhatWeb [13], ffuf [4] e sqlmap [11]
- Vulnerability Mapping: sono stati utilizzati i tool cookies.txt [3], Nessus [8], Nikto2 [9] e Burp Suite DOM Invader [1].
- Target Exploitation: sono stati utilizzati i tool Burp Suite DOM Invader e Repeater [2], e Hashcat [5]
- Target Post-exploitation: sono stati utilizzati i tool LinPEAS [6] e Metasploit [7]

3 | Vulnerability report

L'analisi di FormulaX ha rilevato le seguenti vulnerabilità ad alto rischio:

- Assenza di controlli sull'input degli utenti inviato tramite form. Questo permette molteplici attacchi tra cui esecuzione di comandi malevoli sulla macchina, manipolazione e furto dei dati degli utenti;
- Versione vulnerabile del tool utilizzato per la costruzione del dominio dev-git-auto-update.chatbot.htb. Questo permette l'esecuzione di comandi malevoli sulla macchina;
- Password debole dell'utente Frank_dorky. Questo permette il recupero della password in chiaro e l'impersonificazione di un utente;
- Lettura della configurazione di LibreNMS da parte di utenti non admin. Questo permette il recupero delle credenziali dell'utente kai_relay;
- Permesso agli utenti non admin di eseguire software che richiederebbe privilegi elevati;
- Presenza di vari software che presentano debolezze e che potrebbero essere sfruttati per eseguire azioni riservate agli admin e/o di accedere al sistema in modo malevolo.

Inoltre si riportano debolezze nel sistema che potrebbero creare vulnerabilità e facilitare operazioni malevole:

- Rilevazione del sistema operativo di FormulaX utilizzando opportuni tool. Questo facilita la ricerca di vulnerabilità;
- Rilevazione dei server SSH e HTTP e delle loro versioni utilizzando opportuni tool. Questo facilita la ricerca di vulnerabilità;
- Presenza di informazioni non necessarie nelle risposte HTTP. Questo facilita la ricerca di vulnerabilità e la comprensione del sistema;
- Assenza delle informazioni anti Clickjacking nelle risposte HTTP. Potrebbe essere sfruttato per manipolare il comportamento degli utenti.

4 | Remediation report

La macchina FormulaX possiede un grado di rischio molto elevato, per cercare di mitigare questo fattore è possibile prendere le seguenti contromisure:

- Implementare mediante opportune tecniche il filtraggio dei dati ricevuti attraverso i form delle applicazioni web;
- Aggiornamento di Simple-git all'ultima versione stabile recente 3.25.0;
- Far scegliere agli utenti del sistema password complesse e senza un significato particolare;
- Non permettere agli utenti non admin la lettura e l'esecuzione di file che richiedono privilegi elevati e/o che contengono informazioni sensibili;
- Aggiornare ogni package del sistema alla versione più recente.

5 | Findings summary

Durante l'attività di penetration testing, utilizzando il tool automatico Nessus, sono state individuate 49 vulnerabilità e 66 informazioni che potrebbero generare vulnerabilità in futuro nella macchina target FormulaX. Nessus è stato utilizzato sia senza aver impostato le credenziali SSH degli utenti sia con le credenziali impostate (ottenute nella fase di Target Exploitation), di seguito verranno riportate le vulnerabilità rilevate durante la scansione con le credenziali SSH impostate, siccome risulta più completa e dettagliata. Le vulnerabilità individuate sono state suddivise in quattro classi in base alla loro gravità:

- CRITICAL: vulnerabilità che potrebbero avere un impatto elevato e che possono consentire ad un utente malintenzionato di ottenere un controllo completo o parziale del sistema;
- HIGH: vulnerabilità che richiedono determinati requisiti per poter essere sfruttate e hanno un impatto relativamente alto sul sistema;
- MEDIUM: vulnerabilità non semplici da sfruttare e che, nella maggior parte dei casi, non hanno un impatto diretto molto significativo;
- LOW: vulnerabilità che hanno un impatto poco significativo e che hanno una bassa probabilità di essere sfruttate e, pertanto, non rappresentano, nell'immediato, una minaccia rilevante per il sistema;
- INFO: non sono vulnerabilità ma sono informazioni su configurazioni e su software che nel futuro potrebbero generare delle vulnerabilità;

La tabella seguente mostra il numero di vulnerabilità individuate per ogni categoria:

	CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
Numero vulnerabilità Nessus	8	26	12	3	63	115

Di seguito è mostrato anche un grafico a torta per avere una visione più dettagliata sul numero di vulnerabilità presenti:

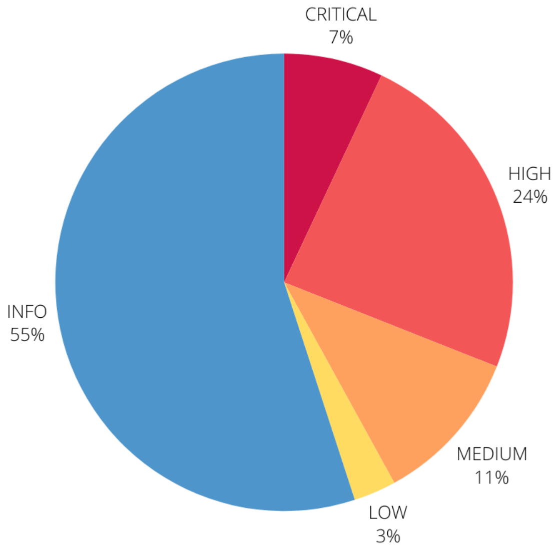

Figure 5.1: Risultati ottenuti con Nessus

Le vulnerabilità rilevate in maniera automatica da Nessus sono dovute alla presenza di package software non aggiornati. A queste bisogna aggiungere le vulnerabilità rilevate in maniera manuale e per via di altri tool (non rilevate da Nessus).
In particolare nella classe CRITICAL rientrano:

- L'assenza di controlli sull'input ricevuto via form: l'applicazione risulta vulnerabile a DOM XSS, CSRF ed esecuzione remota di codice;
- Versione vulnerabile di Simple-git: permette esecuzione remota di codice, CVE-2022-25912;

Nella sezione HIGH rientrano:

- Permesso agli utenti non admin di eseguire e leggere file che richiederebbero permessi elevati;
- Le vulnerabilità rilevate da LinPEAS: CVE-2021-4034, CVE-2021-3156, CVE-2021-22555 e CVE-2022-0847

Nella sezione MEDIUM rientrano:

- Aggiornamento packages a versioni stabili recenti;
- Credenziali degli utenti troppo semplici.

Nella sezione INFO e LOW rientra tutto ciò che riguarda la presenza di informazioni nelle risposte HTTP, la possibilità di Clickjacking e la rilevazione del sistema operativo. L'assegnazione in classi di queste vulnerabilità è avvenuta considerando l'impatto che potrebbero avere su FormulaX.

6 | Detailed summary

In questa sezione sono presenti le descrizioni dettagliate delle vulnerabilità rilevate da Nessus, da LinPEAS e usando metodi manuali. Vengono riportate anche debolezze che nel caso di FormulaX diventano vulnerabilità con un impatto significante.

6.1 | Critical

<table>
<tr><td colspan="3"><b>Titolo:</b>Improper Control of Generation of Code ('Code Injection')</td></tr>
<tr><td><b>Classe</b></td><td><b>Weakness ID</b></td><td></td></tr>
<tr><td>critical</td><td>94</td><td></td></tr>
<tr><td colspan="3"><b>Description:</b> The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Backend implementation of user input controls.</td></tr>
</table>

Link: https://cwe.mitre.org/data/definitions/94.html

<table>
<tr><td colspan="3"><b>Titolo:</b> Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</td></tr>
<tr><td><b>Classe</b></td><td><b>Weakness ID</b></td><td></td></tr>
<tr><td>critical</td><td>79</td><td></td></tr>
<tr><td colspan="3"><b>Description:</b> The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Backend implementation of user input controls.</td></tr>
</table>

Link: https://cwe.mitre.org/data/definitions/79.html

<table>
<tr><td colspan="3"><b>Titolo:</b> Simple-git <3.15 vulnerable to Remote Code Execution</td></tr>
<tr><td><b>Classe</b></td><td><b>CVE ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>critical</td><td>CVE-2022-25912</td><td>9.8</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> Vulnerable to Remote Code Execution (RCE) when enabling the ext transport protocol, which makes it exploitable via clone() method</td></tr>
<tr><td colspan="3"><b>Description:</b> The package simple-git before 3.15.0 are vulnerable to Remote Code Execution (RCE) when enabling the ext transport protocol, which makes it exploitable via clone() method. This vulnerability exists due to an incomplete fix of [CVE-2022-24066](https://security.snyk.io/vuln/SNYK-JS-SIMPLEGIT-2434306).</td></tr>
<tr><td colspan="3"><b>Solution:</b> Upgrade to Simple-git version 3.25.0.</td></tr>
</table>

Link: https://www.tenable.com/cve/CVE-2022-25912

Titolo: Node.js 16.x < 16.20.2 / 18.x < 18.17.1 / 20.x < 20.5.1 Multiple Vulnerabilities (Wednesday August 09 2023 Security Releases).		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
critical	179692	9.8
Synopsis: Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.		
Description: The version of Node.js installed on the remote host is prior to 16.20.2, 18.17.1, 20.5.1. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday August 09 2023 Security Releases advisory:		
Solution: Upgrade to Node.js version 16.20.22 / 18.17.1 / 20.5.1 or later.		

Link: https://www.tenable.com/plugins/nessus/179692

Titolo: Node.js 18.x < 18.18.2 / 20.x < 20.8.1 Multiple Vulnerabilities (Friday October 13 2023 Security Releases).		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
critical	183390	9.8
Synopsis: Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.		
Description: The version of Node.js installed on the remote host is prior to 18.18.2, 20.8.1. It is, therefore, affected by multiple vulnerabilities as referenced in the Friday October 13 2023 Security Releases advisory.		
Solution: Upgrade to Node.js version 18.18.2 / 20.8.1 or later.		

Link: https://www.tenable.com/plugins/nessus/183390

Titolo: Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6725-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
critical	193084	9.8
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6725-1 advisory.		
Solution: Update the affected kernel package.		

Link: https://www.tenable.com/plugins/nessus/193084

Titolo: Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities (USN-6736-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
critical	193362	9.8
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6736-1 advisory.		
Solution: Update the affected klibc-utils, libklibc and / or libklibc-dev packages.		

Link: https://www.tenable.com/plugins/nessus/193362

Titolo: Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GNU C Library vulnerability (USN-6737-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
critical	193515	9.1
Synopsis: The remote Ubuntu host is missing a security update.		
Description: The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6737-1 advisory.		
Solution: Update the affected packages.		

Link: https://www.tenable.com/plugins/nessus/193515

Titolo: Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less vulnerability (USN-6756-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
critical	194474	9.8
Synopsis: The remote Ubuntu host is missing a security update.		
Description: The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. host has a package installed that is affected by a vulnerability as referenced in the USN-6756-1 advisory.		
Solution: Update the affected less package.		

Link: https://www.tenable.com/plugins/nessus/194474

Titolo: Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Git vulnerabilities (USN-6793-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
critical	198042	9
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6793-1 advisory.		
Solution: Update the affected packages.		

Link: https://www.tenable.com/plugins/nessus/198042

Titolo: Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : PyMySQL vulnerability (USN-6801-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
critical	198153	9.8
Synopsis: The remote Ubuntu host is missing a security update.		
Description: The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-6801-1 advisory.		
Solution: Update the affected python3-pymysql package.		

Link: https://www.tenable.com/plugins/nessus/198153

6.2 | High

Titolo: Ubuntu 18.04 LTS / 20.04 LTS : PolicyKit vulnerability (USN-5252-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	157112	7.8
Synopsis: The remote Ubuntu host is missing a security update.		
Description: The remote Ubuntu 18.04 LTS / 20.04 LTS / 21.10 host has packages installed that are affected by a vulnerability as referenced in the USN-5252-1 advisory.		
Solution: Update the affected packages.		
Exploitable With: CVE-2021-4034		

Link: https://www.tenable.com/plugins/nessus/157112

Titolo: Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Sudo vulnerabilities (USN-4705-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	145463	7.8
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4705-1 advisory.		
Solution: Update the affected sudo and / or sudo-ldap packages.		
Exploitable With: CVE-2021-23239		

Link: https://www.tenable.com/plugins/nessus/145463

Titolo: Ubuntu 16.04 ESM : Linux kernel vulnerability (USN-5039-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	152536	7.8
Synopsis: The remote Ubuntu host is missing a security update.		
Description: The remote Ubuntu 16.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-5039-1 advisory.		
Solution: Update the affected kernel package.		
Exploitable With: CVE-2021-22555		

Link: https://www.tenable.com/plugins/nessus/152536

Titolo: Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5317-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	158731	7.8
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5317-1 advisory.		
Solution: Update the affected kernel package.		
Exploitable With: CVE-2022-0001		

Link: https://www.tenable.com/plugins/nessus/158731 s

Titolo: Incorrect Privilege Assignment		
Classe	**Weakness ID**	
high	266	
Description: A product incorrectly assigns a privilege to a particular actor, creating an unintended sphere of control for that actor.		
Solution: Adopt the least privilege strategy		

Link: https://cwe.mitre.org/data/definitions/266.html

Titolo: Node.js 16.x < 16.20.1 / 18.x < 18.16.1 / 20.x < 20.3.1 Multiple Vulnerabilities (Tuesday June 20 2023 Security Releases).		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	177518	7.5
Synopsis: Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.		
Description: The version of Node.js installed on the remote host is prior to 16.20.1, 18.16.1, 20.3.1. It is, therefore, affected by multiple vulnerabilities as referenced in the Tuesday June 20 2023 Security Releases advisory.		
Solution: Upgrade to Node.js version 16.20.1 / 18.16.1 / 20.3.1 or later.		

Link: https://www.tenable.com/plugins/nessus/177518

Titolo: Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 ESM / 23.04 : ImageMagick vulnerabilities (USN-6200-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	177934	7.8
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 ESM / 22.10 / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6200-1 advisory.		
Solution: Update the affected packages.		

Link: https://www.tenable.com/plugins/nessus/177934

Titolo: Node.js 18.x < 18.19.1 / 20.x < 20.11.1 / 21.x < 21.6.2 Multiple Vulnerabilities (Wednesday February 14 2024 Security Releases).		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	190856	7.9
Synopsis: Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.		
Description: The version of Node.js installed on the remote host is prior to 18.19.1, 20.11.1, 21.6.2. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday February 14 2024 Security Releases advisory.		
Solution: Upgrade to Node.js version 18.19.1 / 20.11.1 / 21.6.2 or later.		

Link: https://www.tenable.com/plugins/nessus/190856

Titolo: Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : libde265 vulnerabilities (USN-6677-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	191560	8.8
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6677-1 advisory.		
Solution: Update the affected libde265-0, libde265-dev and / or libde265-examples packages.		

Link: https://www.tenable.com/plugins/nessus/191560

Titolo: Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6686-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	191737	7.8
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6686-1 advisory.		
Solution: Update the affected kernel package.		

Link: https://www.tenable.com/plugins/nessus/191737

Titolo: Ubuntu 22.04 LTS / 23.10 : Expat vulnerabilities (USN-6694-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	192118	7.5
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6694-1 advisory.		
Solution: Update the affected expat, libexpat1 and / or libexpat1-dev packages.		

Link: https://www.tenable.com/plugins/nessus/192118

Titolo: Ubuntu 22.04 LTS : Bash vulnerability (USN-6697-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	192198	7.8
Synopsis: The remote Ubuntu host is missing a security update.		
Description: The remote Ubuntu 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6697-1 advisory.		
Solution: Update the affected bash, bash-builtins and / or bash-static packages.		

Link: https://www.tenable.com/plugins/nessus/192198

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Vim vulnerability (USN-6698-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>high</td><td>192219</td><td>7.8</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing a security update.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6698-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected packages.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/192219

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6704-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>high</td><td>192312</td><td>7.8</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing one or more security updates.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6704-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected kernel package.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/192312

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Graphviz vulnerability (USN-6708-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>high</td><td>192397</td><td>7.8</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing a security update.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6708-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected packages.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/192397

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : curl vulnerabilities (USN-6718-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>high</td><td>192621</td><td>7.5</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing one or more security updates.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6718-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected packages.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/192621

Titolo: Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : util-linux vulnerability (USN-6719-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	192629	8.8
Synopsis: The remote Ubuntu host is missing a security update.		
Description: The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6719-1 advisory.		
Solution: Update the affected packages.		

Link: https://www.tenable.com/plugins/nessus/192629

Titolo: Node.js 18.x < 18.20.1 / 20.x < 20.12.1 / 21.x < 21.7.2 Multiple Vulnerabilities (Wednesday, April 3, 2024 Security Releases).		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	192945	8.2
Synopsis: Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.		
Description: The version of Node.js installed on the remote host is prior to 18.20.1, 20.12.1, 21.7.2. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday, April 3, 2024 Security Releases advisory.		
Solution: Upgrade to Node.js version 18.20.1 / 20.12.1 / 21.7.2 or later.		

Link: https://www.tenable.com/plugins/nessus/192945

Titolo: Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : util-linux vulnerability (USN-6719-2)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	193159	8.4
Synopsis: The remote Ubuntu host is missing a security update.		
Description: The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6719-2 advisory.		
Solution: Update the affected packages.		

Link: https://www.tenable.com/plugins/nessus/193159

Titolo: Node.js 18.x < 18.20.2 / 20.x < 20.12.2 / 21.x < 21.7.3 Multiple Vulnerabilities (Wednesday, April 10, 2024 Security Releases).		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	193580	8.4
Synopsis: Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.		
Description: The version of Node.js installed on the remote host is prior to 18.20.2, 20.12.2, 21.7.3. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday, April 10, 2024 Security Releases advisory.		
Solution: Upgrade to Node.js version 18.20.2 / 20.12.2 / 21.7.3 or later.		

Link: https://www.tenable.com/plugins/nessus/193580

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6742-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>high</td><td>193595</td><td>7.8</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing one or more security updates.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6742-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected kernel package.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/193595

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : nghttp2 vulnerabilities (USN-6754-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>high</td><td>193905</td><td>7.5</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing one or more security updates.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6754-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected packages.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/193905

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6766-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>high</td><td>195134</td><td>7.8</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing one or more security updates.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6766-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected kernel package.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/195134

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GLib vulnerability (USN-6768-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>high</td><td>195216</td><td>8.1</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing a security update.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6768-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected packages.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/195216

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibreOffice vulnerability (USN-6789-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>high</td><td>198045</td><td>8.8</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing a security update.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6789-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected packages.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/198045

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Intel Microcode vulnerabilities (USN-6797-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>high</td><td>198069</td><td>7.9</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing one or more security updates.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6797-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected intel-microcode package.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/198069

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GStreamer Base Plugins vulnerability (USN-6798-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>high</td><td>198070</td><td>7.8</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing a security update.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6798-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected packages.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/198070

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GNU C Library vulnerabilities (USN-6804-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>high</td><td>198244</td><td>7.6</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing one or more security updates.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6804-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected packages.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/198244

Titolo: Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GDK-PixBuf vulnerability (USN-6806-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	200128	7.8
Synopsis: The remote Ubuntu host is missing a security update.		
Description: The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6806-1 advisory.		
Solution: Update the affected packages.		

Link: https://www.tenable.com/plugins/nessus/200128

Titolo: Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6820-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	200223	8
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6820-1 advisory.		
Solution: Update the affected kernel package.		

Link: https://www.tenable.com/plugins/nessus/200223

Titolo: Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : GIFLIB vulnerabilities (USN-6824-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
high	200257	8.8
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6824-1 advisory.		
Solution: Update the affected giflib-tools, libgif-dev and / or libgif7 packages.		

Link: https://www.tenable.com/plugins/nessus/200257

6.3 | Medium

Titolo: Use of Weak Credentials		
Classe	**Weakness ID**	
medium	1391	
Description: The product uses weak credentials (such as a default key or hard-coded password) that can be calculated, derived, reused, or guessed by an attacker.		
Solution: choose long passwords with symbols, upper and lower case letters		

Link: https://cwe.mitre.org/data/definitions/1391.html

Titolo: Ubuntu 20.04 ESM / 22.04 ESM : OpenEXR vulnerabilities (USN-5620-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
medium	183721	6.5
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 20.04 ESM / 22.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5620-1 advisory.		
Solution: Update the affected packages.		

Link: https://www.tenable.com/plugins/nessus/183721

Titolo: Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : ImageMagick vulnerability (USN-6621-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
medium	189915	5.5
Synopsis: The remote Ubuntu host is missing a security update.		
Description: The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6621-1 advisory.		
Solution: Update the affected packages.		

Link: https://www.tenable.com/plugins/nessus/189915

Titolo: Node.js Module node-tar < 6.2.1 DoS		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
medium	192685	6.5
Synopsis: A module in the Node.js JavaScript run-time environment is affected by a denial of service vulnerability.		
Description: In the nodejs module node-tar prior to version 6.2.1, there is no validation of the number of folders created while unpacking a file. As a result, an attacker can use a malicious file to exhaust the CPU and memory on the host and crash the nodejs client.		
Solution: Upgrade to node-tar version 6.2.1 or later.		

Link: https://www.tenable.com/plugins/nessus/192685

Titolo: Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : NSS vulnerabilities (USN-6727-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
medium	193171	6.5
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6727-1 advisory.		
Solution: Update the affected libnss3, libnss3-dev and / or libnss3-tools packages.		

Link: https://www.tenable.com/plugins/nessus/193171

Titolo: Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GnuTLS vulnerabilities (USN-6733-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
medium	193341	5.3
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6733-1 advisory.		
Solution: Update the affected packages.		

Link: https://www.tenable.com/plugins/nessus/193341

Titolo: Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GNU cpio vulnerabilities (USN-6755-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
medium	194475	4.9
Synopsis: The remote Ubuntu host is missing a security update.		
Description: The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6755-1 advisory.		
Solution: Update the affected cpio and / or cpio-win32 packages.		

Link: https://www.tenable.com/plugins/nessus/194475

Titolo: Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : PHP vulnerabilities (USN-6757-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
medium	194504	5.5
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6757-1 advisory.		
Solution: Update the affected packages.		

Link: https://www.tenable.com/plugins/nessus/194504

Titolo: Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : PHP vulnerabilities (USN-6757-2)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
medium	194949	5.5
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6757-2 advisory.		
Solution: Update the affected packages.		

Link: https://www.tenable.com/plugins/nessus/194949

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : libde265 vulnerability (USN-6764-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>medium</td><td>195117</td><td>5.5</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing a security update.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6764-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected libde265-0, libde265-dev and / or libde265-examples packages.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/195117

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6775-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>medium</td><td>197214</td><td>4.3</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing one or more security updates.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6775-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected kernel package.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/197214

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : MySQL vulnerabilities (USN-6823-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>medium</td><td>200259</td><td>4.9</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing one or more security updates.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6823-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected packages.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/200259

<table>
<tr><td colspan="3"><b>Titolo:</b> Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibTIFF vulnerability (USN-6827-1)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>medium</td><td>200307</td><td>5.5</td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote Ubuntu host is missing a security update.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6827-1 advisory.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Update the affected packages.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/200307

6.4 | Low

Titolo: ICMP Timestamp Request Remote Date Disclosure		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
low	10114	2.1
Synopsis: It is possible to determine the exact time set on the remote host.		
Description: The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.		
Solution: Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).		

Link: https://www.tenable.com/plugins/nessus/10114

Titolo: OpenJDK 8 <= 8u402 / 11.0.0 <= 11.0.22 / 17.0.0 <= 17.0.10 / 21.0.0 <= 21.0.2 / 22.0.0 <= 22.0.0 Multiple Vulnerabilities (2024-04-16		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
low	193405	3.7
Synopsis: OpenJDK is affected by multiple vulnerabilities.		
Description: The version of OpenJDK installed on the remote host is prior to 8 <= 8u402 / 11.0.0 <= 11.0.22 / 17.0.0 <= 17.0.10 / 21.0.0 <= 21.0.2 / 22.0.0 <= 22.0.0. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024-04-16 advisory.		
Solution: Upgrade to an OpenJDK version greater than 8u402 / 11.0.22 / 17.0.10 / 21.0.2 / 22.0.0		

Link: https://www.tenable.com/plugins/nessus/193405

Titolo: Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : OpenJDK 11 vulnerabilities (USN-6811-1)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
low	200142	3.7
Synopsis: The remote Ubuntu host is missing one or more security updates.		
Description: The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6811-1 advisory.		
Solution: Update the affected packages.		

Link: https://www.tenable.com/plugins/nessus/200142

6.5 | Info

Titolo: HTTP Server Type and Version		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	10107	
Synopsis: A web server is running on the remote host.		
Description: This plugin attempts to determine the type and the version of the remote web server.		

Link: https://www.tenable.com/plugins/nessus/10107

Titolo: SSH Commands Require Privilege Escalation		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	102094	
Synopsis: This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them.		
Description: This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them. Either privilege escalation credentials were not provided, or the command failed to run with the provided privilege escalation credentials.		

Link: https://www.tenable.com/plugins/nessus/102094

Titolo: SSH Server Type and Version Information		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	10267	
Synopsis: An SSH server is listening on this port.		
Description: It is possible to obtain information about the remote SSH server by sending an empty authentication request.		

Link: https://www.tenable.com/plugins/nessus/10267

Titolo: Traceroute Information		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	10287	
Synopsis: It was possible to obtain traceroute information.		
Description: Makes a traceroute to the remote host.		

Link: https://www.tenable.com/plugins/nessus/10287

Titolo: nginx HTTP Server Detection		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	106375	
Synopsis: The nginx HTTP server was detected on the remote host.		
Description: Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.		

Link: https://www.tenable.com/plugins/nessus/106375

Titolo: SSH Protocol Versions Supported		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	10881	
Synopsis: A SSH server is running on the remote host.		
Description: This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.		

Link: https://www.tenable.com/plugins/nessus/10881

Titolo: Target Credential Issues by Authentication Protocol - Insufficient Privilege		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	110385	
Synopsis: Nessus was able to log in to the remote host using the provided credentials. The provided credentials were not sufficient to complete all requested checks.		
Description: Nessus was able to execute credentialed checks because it was possible to log in to the remote host using provided credentials, however the credentials were not sufficiently privileged to complete all requested checks.		

Link: https://www.tenable.com/plugins/nessus/110385

Titolo: Unix / Linux Running Processes Information		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	110483	
Synopsis: Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.		
Description: Generated report details the running processes on the target machine at scan time.		

Link: https://www.tenable.com/plugins/nessus/110483

Titolo: OS Security Patch Assessment Available		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	117887	
Synopsis: Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.		
Description: Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.		

Link: https://www.tenable.com/plugins/nessus/117887

Titolo: OS Identification		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	11936	
Synopsis: It is possible to guess the remote operating system.		
Description: Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.		

Link: https://www.tenable.com/plugins/nessus/11936

<table>
<tr><td colspan="3"><b>Titolo:</b> Host Fully Qualified Domain Name (FQDN) Resolution</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>info</td><td>12053</td><td></td></tr>
<tr><td colspan="3"><b>Synopsis:</b> It was possible to resolve the name of the remote host.</td></tr>
<tr><td colspan="3"><b>Description:</b> Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/12053

<table>
<tr><td colspan="3"><b>Titolo:</b> MariaDB Client/Server Installed (Linux)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>info</td><td>130626</td><td></td></tr>
<tr><td colspan="3"><b>Synopsis:</b> One or more MariaDB server or client versions are available on the remote Linux host.</td></tr>
<tr><td colspan="3"><b>Description:</b> One or more MariaDB server or client versions have been detected on the remote Linux host.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/130626

<table>
<tr><td colspan="3"><b>Titolo:</b> nginx Installed (Linux/UNIX)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>info</td><td>136340</td><td></td></tr>
<tr><td colspan="3"><b>Synopsis:</b> NGINX is installed on the remote Linux / Unix host.</td></tr>
<tr><td colspan="3"><b>Description:</b> NGINX, a web server with load balancing capabilities, is installed on the remote Linux / Unix host.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/136340

<table>
<tr><td colspan="3"><b>Titolo:</b> Target Credential Status by Authentication Protocol - Valid Credentials Provided</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>info</td><td>141118</td><td></td></tr>
<tr><td colspan="3"><b>Synopsis:</b> Valid credentials were provided for an available authentication protocol.</td></tr>
<tr><td colspan="3"><b>Description:</b> Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/141118

Titolo: Netstat Portscanner (SSH)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	14272	
Synopsis: Remote open ports can be enumerated via SSH.		
Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.		

Link: https://www.tenable.com/plugins/nessus/14272

Titolo: Java Detection and Identification (Linux / Unix)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	147817	
Synopsis: Java is installed on the remote Linux / Unix host.		
Description: One or more instances of Java are installed on the remote Linux / Unix host. This may include private JREs bundled with the Java Development Kit (JDK).		

Link: https://www.tenable.com/plugins/nessus/147817

Titolo: OpenJDK Java Detection (Linux / Unix)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	148373	
Synopsis: A distribution of Java is installed on the remote Linux / Unix host.		
Description: One or more instances of OpenJDK Java are installed on the remote host. This may include private JREs bundled with the Java Development Kit (JDK).		

Link: https://www.tenable.com/plugins/nessus/148373

Titolo: SSH Password Authentication Accepted		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	149334	
Synopsis: The SSH server on the remote host accepts password authentication.		
Description: The SSH server on the remote host accepts password authentication.		

Link: https://www.tenable.com/plugins/nessus/149334

Titolo: Libgcrypt Installed (Linux/UNIX)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	151883	
Synopsis: Libgcrypt is installed on this host.		
Description: Libgcrypt, a cryptography library, was found on the remote host.		

Link: https://www.tenable.com/plugins/nessus/151883

<table>
<tr><td colspan="3"><b>Titolo:</b> Unix Software Discovery Commands Available</td></tr>
<tr><th>Classe</th><th>Nessus Plugin ID</th><th>CVSS v3 Base Score</th></tr>
<tr><td>info</td><td>152742</td><td></td></tr>
<tr><td colspan="3"><b>Synopsis:</b> Nessus was able to log in to the remote host using the provided credentials and is able to execute all commands used to find unmanaged software.</td></tr>
<tr><td colspan="3"><b>Description:</b> Nessus was able to determine that it is possible for plugins to find and identify versions of software on the target host. Software that is not managed by the operating system is typically found and characterized using these commands. This was measured by running commands used by unmanaged software plugins and validating their output against expected results.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/152742

<table>
<tr><td colspan="3"><b>Titolo:</b> SSH SHA-1 HMAC Algorithms Enabled</td></tr>
<tr><th>Classe</th><th>Nessus Plugin ID</th><th>CVSS v3 Base Score</th></tr>
<tr><td>info</td><td>153588</td><td></td></tr>
<tr><td colspan="3"><b>Synopsis:</b> The remote SSH server is configured to enable SHA-1 HMAC algorithms.</td></tr>
<tr><td colspan="3"><b>Description:</b> The remote SSH server is configured to enable SHA-1 HMAC algorithms.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/153588

<table>
<tr><td colspan="3"><b>Titolo:</b> Linux Mounted Devices</td></tr>
<tr><th>Classe</th><th>Nessus Plugin ID</th><th>CVSS v3 Base Score</th></tr>
<tr><td>info</td><td>157358</td><td></td></tr>
<tr><td colspan="3"><b>Synopsis:</b> Use system commands to obtain the list of mounted devices on the target machine at scan time.</td></tr>
<tr><td colspan="3"><b>Description:</b> Report the mounted devices information on the target machine at scan time using the following commands.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/157358

<table>
<tr><td colspan="3"><b>Titolo:</b> OpenSSL Installed (Linux)</td></tr>
<tr><th>Classe</th><th>Nessus Plugin ID</th><th>CVSS v3 Base Score</th></tr>
<tr><td>info</td><td>168007</td><td></td></tr>
<tr><td colspan="3"><b>Synopsis:</b> OpenSSL was detected on the remote Linux host.</td></tr>
<tr><td colspan="3"><b>Description:</b> OpenSSL was detected on the remote Linux host.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/168007

<table>
<tr><td colspan="3"><b>Titolo:</b> Filepaths contain Dangerous characters (Linux)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>info</td><td>168982</td><td></td></tr>
<tr><td colspan="3"><b>Synopsis:</b> This Tenable product detected files or paths on the scanned Unix-like system which contain characters with command injection or privilege escalation potential.</td></tr>
<tr><td colspan="3"><b>Description:</b> This Tenable product detected files or paths on the scanned Unix-like system which contain characters with command injection or privilege escalation potential. Although almost any character is valid for an entry in this kind of filesystem, such as semicolons, use of some of them may lead to problems or security compromise when used in further commands.</td></tr>
<tr><td colspan="3"><b>Solution:</b> Rename these files or folders to not include dangerous characters.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/168982

<table>
<tr><td colspan="3"><b>Titolo:</b> Enumerate the Network Interface configuration via SSH</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>info</td><td>170170</td><td></td></tr>
<tr><td colspan="3"><b>Synopsis:</b> Nessus was able to parse the Network Interface data on the remote host.</td></tr>
<tr><td colspan="3"><b>Description:</b> Nessus was able to parse the Network Interface data on the remote host.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/170170

<table>
<tr><td colspan="3"><b>Titolo:</b> IP Assignment Method Detection</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>info</td><td>171410</td><td></td></tr>
<tr><td colspan="3"><b>Synopsis:</b> Enumerates the IP address assignment method(static/dynamic).</td></tr>
<tr><td colspan="3"><b>Description:</b> Enumerates the IP address assignment method(static/dynamic).</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/171410

<table>
<tr><td colspan="3"><b>Titolo:</b> Node.js Installed (Linux / UNIX)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>info</td><td>178771</td><td></td></tr>
<tr><td colspan="3"><b>Synopsis:</b> Node.js is installed on the remote Linux / UNIX host.</td></tr>
<tr><td colspan="3"><b>Description:</b> Node.js is installed on the remote Linux / UNIX host.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/178771

<table>
<tr><td colspan="3"><b>Titolo:</b> Node.js Modules Installed (Linux)</td></tr>
<tr><td><b>Classe</b></td><td><b>Nessus Plugin ID</b></td><td><b>CVSS v3 Base Score</b></td></tr>
<tr><td>info</td><td>178772</td><td></td></tr>
<tr><td colspan="3"><b>Synopsis:</b> Nessus was able to enumerate one or more Node.js modules installed on the remote host.</td></tr>
<tr><td colspan="3"><b>Description:</b> Nessus was able to enumerate one or more Node.js modules installed on the remote host.</td></tr>
</table>

Link: https://www.tenable.com/plugins/nessus/178772

Titolo: Enumerate the Network Routing configuration via SSH		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	179200	
Synopsis: Nessus was able to retrieve network routing information from the remote host.		
Description: Nessus was able to retrieve network routing information the remote host.		

Link: https://www.tenable.com/plugins/nessus/179200

Titolo: OpenSSH Detection		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	181418	
Synopsis: An OpenSSH-based SSH server was detected on the remote host.		
Description: An OpenSSH-based SSH server was detected on the remote host.		

Link: https://www.tenable.com/plugins/nessus/181418

Titolo: Curl Installed (Linux / Unix)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	182774	
Synopsis: Curl is installed on the remote Linux / Unix host.		
Description: Curl (also known as curl and cURL) is installed on the remote Linux / Unix host.		

Link: https://www.tenable.com/plugins/nessus/182774

Titolo: libcurl Installed (Linux / Unix)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	182848	
Synopsis: libcurl is installed on the remote Linux / Unix host.		
Description: libcurl is installed on the remote Linux / Unix host.		

Link: https://www.tenable.com/plugins/nessus/182848

Titolo: VMWare Tools or Open VM Tools Installed (Linux)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	186361	
Synopsis: VMWare Tools or Open VM Tools were detected on the remote Linux host.		
Description: VMWare Tools or Open VM Tools were detected on the remote Linux host.		

Link: https://www.tenable.com/plugins/nessus/186361

Titolo: Tukaani XZ Utils Installed (Linux / Unix)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	192709	
Synopsis: Tukaani XZ Utils is installed on the remote Linux / Unix host.		
Description: Tukaani XZ Utils is installed on the remote Linux / Unix host.		

Link: https://www.tenable.com/plugins/nessus/192709

Titolo: Linux Time Zone Information		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	193143	
Synopsis: Nessus was able to collect and report time zone information from the remote host.		
Description: Nessus was able to collect time zone information from the remote Linux host.		
Solution: None		

Link: https://www.tenable.com/plugins/nessus/193143

Titolo: Ubuntu 20.04 LTS / 22.04 LTS : NSS regression (USN-6727-2)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	193233	
Synopsis: The remote Ubuntu host is missing a security update.		
Description: The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6727-2 advisory.		
Solution: Update the affected libnss3, libnss3-dev and / or libnss3-tools packages.		

Link: https://www.tenable.com/plugins/nessus/193233

Titolo: Nessus Scan Information		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	19506	
Synopsis: This plugin displays information about the Nessus scan.		
Description: This plugin displays, for each tested host, information about the scan itself :		

Link: https://www.tenable.com/plugins/nessus/19506

Titolo: VMware Virtual Machine Detection		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	20094	
Synopsis: The remote host is a VMware virtual machine.		
Description: According to the MAC address of its network adapter, the remote host is a VMware virtual machine.		
Solution: Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.		

Link: https://www.tenable.com/plugins/nessus/20094

Titolo: Software Enumeration (SSH)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	22869	
Synopsis: It was possible to enumerate installed software on the remote host via SSH.		
Description: Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).		
Solution: Remove any software that is not in compliance with your organization's acceptable use and security policies.		

Link: https://www.tenable.com/plugins/nessus/22869

Titolo: Service Detection		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	22964	
Synopsis: The remote service could be identified.		
Description: Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.		

Link: https://www.tenable.com/plugins/nessus/22964

Titolo: HyperText Transfer Protocol (HTTP) Information		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	24260	
Synopsis: Some information about the remote HTTP configuration can be extracted.		
Description: This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...		

Link: https://www.tenable.com/plugins/nessus/24260

Titolo: Enumerate IPv6 Interfaces via SSH		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	25202	
Synopsis: Nessus was able to enumerate the IPv6 interfaces on the remote host.		
Description: Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.		
Solution: Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.		

Link: https://www.tenable.com/plugins/nessus/25202

Titolo: Enumerate IPv4 Interfaces via SSH		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	25203	
Synopsis: Nessus was able to enumerate the IPv4 interfaces on the remote host.		
Description: Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.		
Solution: Disable any unused IPv4 interfaces.		

Link: https://www.tenable.com/plugins/nessus/25203

Titolo: TCP/IP Timestamps Supported		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	25220	
Synopsis: The remote service implements TCP timestamps.		
Description: The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.		

Link: https://www.tenable.com/plugins/nessus/25220

Titolo: Enumerate MAC Addresses via SSH		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	33276	
Synopsis: Nessus was able to enumerate MAC addresses on the remote host.		
Description: Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.		
Solution: Disable any unused interfaces.		

Link: https://www.tenable.com/plugins/nessus/33276

Titolo: BIOS Info (SSH)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	34098	
Synopsis: BIOS info could be read.		
Description: Using SMBIOS and UEFI, it was possible to get BIOS info.		

Link: https://www.tenable.com/plugins/nessus/34098

Titolo: Ethernet Card Manufacturer Detection		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	35716	
Synopsis: The manufacturer can be identified from the Ethernet OUI.		
Description: Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.		

Link: https://www.tenable.com/plugins/nessus/35716

Titolo: Backported Security Patch Detection (SSH)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	39520	
Synopsis: Security patches are backported.		
Description: Security patches may have been 'backported' to the remote SSH server without changing its version number.		

Link: https://www.tenable.com/plugins/nessus/39520

Titolo: Reachable IPv6 address		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	45405	
Synopsis: The remote host may be reachable from the Internet.		
Description: Although this host was scanned through a private IPv4 or local scope IPv6 address, some network interfaces are configured with global scope IPv6 addresses. Depending on the configuration of the firewalls and routers, this host may be reachable from Internet.		
Solution: Disable IPv6 if you do not actually using it.		

Link: https://www.tenable.com/plugins/nessus/45405

Titolo: Common Platform Enumeration (CPE)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	45590	
Synopsis: It was possible to enumerate CPE names that matched on the remote system.		
Description: By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.		

Link: https://www.tenable.com/plugins/nessus/45590

Titolo: Inconsistent Hostname and IP Address		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	46215	
Synopsis: The remote host's hostname is not consistent with DNS information.		
Description: The name of this machine either does not resolve or resolves to a different IP address.		
Solution: Fix the reverse DNS or host file.		

Link: https://www.tenable.com/plugins/nessus/46215

Titolo: Device Type		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	54615	
Synopsis: It is possible to guess the remote device type.		
Description: Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).		

Link: https://www.tenable.com/plugins/nessus/54615

Titolo: Device Hostname		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	55472	
Synopsis: It was possible to determine the remote system hostname.		
Description: This plugin reports a device's hostname collected via SSH or WMI.		

Link: https://www.tenable.com/plugins/nessus/55472

Titolo: Time of Last System Startup		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	56468	
Synopsis: The system has been started.		
Description: Using the supplied credentials, Nessus was able to determine when the host was last started.		

Link: https://www.tenable.com/plugins/nessus/56468

Titolo: Netstat Connection Information		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	64582	
Synopsis: Nessus was able to parse the results of the 'netstat' command on the remote host.		
Description: The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.		

Link: https://www.tenable.com/plugins/nessus/64582

Titolo: Patch Report		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	66334	
Synopsis: The remote host is missing several patches.		
Description: The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.		
Solution: Install the patches listed below.		

Link: https://www.tenable.com/plugins/nessus/66334

Titolo: SSH Algorithms and Languages Supported		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	70657	
Synopsis: An SSH server is listening on this port.		
Description: This script detects which algorithms and languages are supported by the remote service for encrypting communications.		

Link: https://www.tenable.com/plugins/nessus/70657

Titolo: Ethernet MAC Addresses		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	86420	
Synopsis: This plugin gathers MAC addresses from various sources and consolidates them into a list.		
Description: This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.		

Link: https://www.tenable.com/plugins/nessus/86420

Titolo: SSH SCP Protocol Detection		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	90707	
Synopsis: The remote host supports the SCP protocol over SSH.		
Description: The remote host supports the Secure Copy (SCP) protocol over SSH.		

Link: https://www.tenable.com/plugins/nessus/90707

Titolo: Linux User List Enumeration		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	95928	
Synopsis: Nessus was able to enumerate local users and groups on the remote Linux host.		
Description: Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote Linux host.		
Solution: None		

Link: https://www.tenable.com/plugins/nessus/95928

Titolo: OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	97993	
Synopsis: Information about the remote host can be disclosed via an authenticated session.		
Description: Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.		

Link: https://www.tenable.com/plugins/nessus/97993

7 | References

[1] Burp Suite DOM Invader. https://portswigger.net/burp/documentation/desktop/tools/dom-invader.

[2] Burp Suite Repeater. https://portswigger.net/burp/documentation/desktop/tools/repeater.

[3] cookies.txt. https://addons.mozilla.org/it/firefox/addon/cookies-txt/.

[4] ffuf. https://github.com/ffuf/ffuf.

[5] Hashcat. https://hashcat.net/hashcat/.

[6] LinPEAS. https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS/.

[7] Metasploit. https://www.metasploit.com/.

[8] nessus. https://www.tenable.com/products/nessus.

[9] nikto2. https://github.com/sullo/nikto.

[10] Nmap Network Scanner. https://nmap.org/.

[11] sqlmap. https://sqlmap.org/.

[12] Unicornscan. https://www.kali.org/tools/unicornscan/.

[13] Brendan Coles Andrew Horton. WhatWeb. https://morningstarsecurity.com/research/whatweb.

[14] Joe Testa. ssh-audit. https://github.com/jtesta/ssh-audit.

[15] Michal Zalewski. p0f. https://lcamtuf.coredump.cx/p0f3/.