Pentest report - vmi1331840.contaboserve

Summary

I. Overview

This report presents the results of a vulnerability assessment conducted on **vmi1331840.contaboserver.net** using Python modules. The objective of this assessment is to provide a brief overview of the security posture of the target and identify potential vulnerabilities that could be exploited by attackers.

The main objective of the assessment was to identify vulnerabilities that could be used by attackers to compromise the confidentiality, integrity, or availability of the target. Python modules are used to automate the scanning process and identify potential vulnerabilities in the target.

Date: 2024-05-06 12:55

Target : vmi1331840.contaboserver.net

Type: vulnerability scanner

II. DNS Request

Record name	**Informations and data**
A	[{'address': '167.86.69.86', 'ttl': 86400}]
CNAME	No record found
MX	No record found
NS	No record found
SOA	No record found
TXT	No record found

III. Data about HTTP/HTTPS certificate

Error. Check your domain name or the API website (https://networkcalc.com/api/)

IV. NMAP scan

Port	Service	Version
22	ssh	8.2p1 Ubuntu 4ubuntu0.11
80	http	2.4.41
81	http	2.4.7
443	https	
631	ipp	2.4
5000	http	
8000	http-alt	
8080	http	2.4.41

V. Nikto scan

Web server : Apache/2.4.41 (Ubuntu)

The server doesn't support compression.

Version of software might be found in the following header Server : 2.4.41

Target URL don't use any redirection

Target URL isn't protected by a basic HTTP authentication

The anti-clickjacking X-Frame-Options header is not present.

The X-XSS-Protection header is not defined.

The X-Content-Type-Options header is not set.

VI. Potential vulnerabilities

Port : 22, Service: ssh, Version: 8.2p1 Ubuntu 4ubuntu0.11

- CVE-2012-1577

Port : 80, Service: http, Version: 2.4.41

- CVE-2021-2669
- CVE-2021-3927
- CVE-2022-2272
- CVE-2022-2394
- CVE-2022-3181
- CVE-2021-4479
- CVE-2023-2569
- CVE-2020-1198

Port : 81, Service: http, Version: 2.4.7

- CVE-2021-2669
- CVE-2021-3927
- CVE-2022-2272
- CVE-2022-2394
- CVE-2017-7679
- CVE-2017-3167
- CVE-2022-3181
- CVE-2021-4479
- CVE-2023-2569

Port : 631, Service: ipp, Version: 2.4

- CVE-2022-2669

Port : 8080, Service: http, Version: 2.4.41

- CVE-2021-2669
- CVE-2021-3927
- CVE-2022-2272
- CVE-2022-2394
- CVE-2022-3181
- CVE-2021-4479
- CVE-2023-2569
- CVE-2020-1198

VII. Exploit find

Exploits found for CVE-2016-6515:

Exploit Title	Path
Exploit Title	Path
OpenSSH 7.2 - Denial of Service	linux/dos/40888.py

Exploits found for CVE-2016-1000:

Exploit Title	Path
Exploit Title	Path
Adobe Flash - Sprite Creation Use-	windows/dos/39610.txt
Joomla! Component Huge-IT Portfoli	php/webapps/42597.txt
Joomla! Component Huge-IT Portfoli	php/webapps/42598.txt
Joomla! Component Huge-IT Video Ga	php/webapps/42596.txt
OpenSSH < 7.4 - agent Protocol Arb	linux/remote/40963.txt

Exploits found for CVE-2022-3181:

Exploit Title	Path
Exploit Title	Path
pfBlockerNG 2.1.4_26 - Remote Code	php/webapps/51032.py

Exploits found for CVE-2021-4479:

Exploit Title	Path
Exploit Title	Path
Apache 2.4.x - Buffer Overflow	multiple/webapps/51193.py

Exploits found for CVE-2019-0211:

Exploit Title	Path
Exploit Title	Path
Apache 2.4.17 < 2.4.38 - 'apache2c	linux/local/46676.php

Exploits found for CVE-2016-1001:

Exploit Title	Path
Exploit Title	Path
Adobe Flash - Zlib Codec Heap Over	windows/dos/39609.txt

OpenSSH < 7.4 - 'UsePrivilegeSepar	linux/local/40962.txt

VIII. Recommendations

Keep your systems up-to-date with the latest security patches and updates for all software and services running on your domain or IP address. Vulnerabilities are often discovered and patched by vendors, so it's important to stay current with updates to minimize risk.

We also recommend reviewing the list of links provided in this report, which point to known exploits and vulnerabilities affecting various services. These links can provide additional information and guidance on how to mitigate these specific security risks for your domain or IP address.

By following these recommendations and staying vigilant against emerging security threats, you can help protect your systems and data from unauthorized access and exploitation.