Raport z Testów Penetracyjnych TryHackME "Source"

Michał Lissowski

Tester i autor raportu	Michał Lissowski Michallissowski@gmail.com
Miejsce wykonania	Gdańsk
Data wykonania	06.11.2022
Testowana aplikacja/system	Webmin httpd v. 1.890

Niniejszy dokument jest podsumowaniem testu penetracyjnego wykonanego na https://tryhackme.com/room/source .

Skanowanie : nmap

```
Nmap scan report for ip-10-10-184-229.eu-west-1.compute.internal (10.10.184.229)
Host is up (0.0011s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b7:4c:d0:bd:e2:7b:1b:15:72:27:64:56:29:15:ea:23 (RSA)
|   256 b7:85:23:11:4f:44:fa:22:00:8e:40:77:5e:cf:28:7c (ECDSA)
|_  256 a9:fe:4b:82:bf:89:34:59:36:5b:ec:da:c2:d3:95:ce (EdDSA)
10000/tcp open  http    MiniServ 1.890 (Webmin httpd)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-litespeed-sourcecode-download:
| Litespeed Web Server Source Code Disclosure (CVE-2010-2333)
| /index.php source code:
| <h1>Error - Document follows</h1>
|_<p>This web server is running in SSL mode. Try the URL <a href='https://ip-10-10-184-229.eu-west-1.compute.internal:10000/'>https://ip-10-10-184-229.eu
instead.<br></p>
|_http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)
| http-phpmyadmin-dir-traversal:
|   VULNERABLE:
|   phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2005-3299
|       PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-pl1 allows remote attackers to include local files via the
volving the subform array.
|
|     Disclosure date: 2005-10-nil
|     Extra information:
|       ../../../../../etc/passwd :
|   <h1>Error - Document follows</h1>
|   <p>This web server is running in SSL mode. Try the URL <a href='https://ip-10-10-184-229.eu-west-1.compute.internal:10000/'>https://ip-10-10-184-229.
a> instead.<br></p>
|
|     References:
|       http://www.exploit-db.com/exploits/1244/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3299
|_http-server-header: MiniServ/1.890
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
MAC Address: 02:71:0D:A9:A9:EB (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Opis skanowania

Skanowanie nmapem pokazalo 2 otwarte porty. Port 22 (ssh) oraz port 10000. Na porcie 10000 działa panel logowania aplikacji Webmin w przestarzałej wersji 1.890. Zostały znalezione różne podatności które mogą prowadzić do przejęcia kontroli nad maszyną. Wersja aplikacji znajdująca się na testowanej maszynie jest podatna na backdoora.

Poniżej przedstawiona została tabela z wykrytymi podatnościami

Zagrożenie	Podatność	Opis
Krytyczne	Backdoor Webmin v. 1.890 metasploitable	Mechanizm backdoora umożliwiłby zdalnemu napastnikowi wykonanie złośliwych poleceń z uprawnieniami roota na maszynie z uruchomionym Webminem. Po zhakowaniu tej maszyny osoba atakująca może wykorzystać ją do przeprowadzenia ataków na systemy zarządzane przez Webmin. Za pomocą msfconsole metasploit udało się przejąć kontrole nad maszyną bez żadnych danych logowania i automatycznie uzyskać przywileje "root"
Średni	CVE: 2005-3299	Luka w zabezpieczeniach plików PHP w grab_globals.lib.php w phpMyAdmin 2.6.4 i 2.6.4-pl1 umożliwia zdalnym napastnikom włączenie lokalnych plików za pomocą parametru $__redirect, prawdopodobnie obejmującego tablicę podformularzy. Wpływ na integralność. Modyfikacja niektórych plików systemowych lub informacji jest możliwa, ale atakujący nie ma kontroli nad tym, co może zostać zmodyfikowane lub zakres tego, na co może wpłynąć jest ograniczony. Nie ma żadnych modułów metasploit związanych z tym wpisem CVE

Zagrożenie	Podatność	Opis
Średnie	CVE:2010-2333	LiteSpeed Technologies LiteSpeed Web Server 4.0.x przed 4.0.15 umożliwia zdalnym napastnikom odczytywanie kodu źródłowego skryptów za pomocą żądania HTTP z bajtem null, po którym następuje rozszerzenie pliku .txt Istnieje znaczne ujawnienie informacji. Nie ma żadnych modułów metasploit związanych z tym wpisem CVE

Podsumowanie

W aplikacji wykryto podatności pozwalające między innymi na:

- Ominięcie panelu logowania;

- Przejęcie kontroli nad serwerem;

- Przejęcie kontroli nad dowolnym kontem użytkownika;

- Odczytywanie kodu źródłowego skryptów za pomocą żądania HTTP

Zalecana naprawa oraz zapobieganie

Wymagane jest dokonanie odpowiednich poprawek bezpieczeństwa, aktualizacja oprogamowania do najnowszej wersji aplikacji.

Aktualizowanie procesu kompilacji tak, aby używał tylko zaewidencjonowanego kodu z usługi Github, a nie lokalnego katalogu, który jest zsynchronizowany.

Zmieniono wszystkie hasła i klucze dostępne ze starego systemu kompilacji.

Audytowanie wszystkich checkinów Github w ciągu ostatniego roku w poszukiwaniu zatwierdzeń, które mogły wprowadzić podobne luki.