|  |  |
| --- | --- |
| Describe | Vulnerability |
| Service | ssh |
| Port | 4512 |
| Version | 2.4.18 |
| Severity | Easy |
| Cve id |  |
| Cvss score | 7/10 |
| Remediation | 1. **Outdated Vulnerabilities And Remediation Strategies**  * **Issue:** the vm runs an outdated version of wordpress, which may contain known vulnerabilities. * **Remediation:** * **Regularly Updates:** ensure wordpress core, themes, and plugins are updated promptly to patch known vulnerabilities. * **Security Monitoring:** subscribe to WordPress security advisories to stay informed about new vulnerabilities and patches.  1. **Weak Or Default Credentials**  * **Issue:** the use of weak or default credentials allows attackers to gain unauthorized access through brute-force attacks. * **Remediation:** * **Enforce Strong Password Policies:** implement policies requiring complex passwords and regular changes. * **Limit Login Attempts:** use plugins or configurations that limit the number of failed login attempts to prevent brute-force attacks. * **Implement Two Factor Authentication(2FA):** add an extra layer of security to the login process.  1. **Installation Of Vulnerability Plugins**  * **Issue:** the ability to install plugins like file managers can be exploited to execute arbitrary code or access sensitive files. * **Remediations:** * **Restrict Plugin Installations:** limit the ability to install plugins to trusted administrators. * **Review And Vet Plugins:** only use plugins from reputable sources and regularly review their necessity and security. * **Monitor For Unauthorized Changes:** implement file integrity monitor to detect unauthorized modifications.  1. **Presence Of SUID Binaries With Privilege Escalation Potential**  * **Issue:** SUID (set user id) binaries can be exploited to escalate privilages of misconfigured. * **Remediation:** * **Audit SUID Binaries:** regularly check for unnecessary SUID binaries and remove the SUID bit where it’s not required. * **Apply Least Privileges Principle:** Ensure users have only the premissions necessary for their roles. * **Monitor For Unauthorized Changes:** implementmonitoring to detect changes in files permission and ownership.  1. **Exposer Of Sensitive Configuration Files**  * **Issue:** access to files like *wp-config.php* can reveal database credentials and other sensitive information. * **Remediation:** * **Secure File Permissions:** set appropriate file permissions to restrict access to sensitive files. * **Move Configuration Files Outside Web Root:** place configuration files outside the publicly accessible directories when possible. * **Disable Directory Listing:** prevent the web server from listing directory contents. |
| POC | Step 1  First I find our ip in kali    Now I find target ip with netdiscover    As you see I get ip so now I do nmap for getting open ports    As you see I get 80 & 4512 (http & ssh)  Step 2  Now I look at website (http) for getting some information    Here the website “coldbox” so now I start finding some sensitive information    I get login page of wordpress I get hint this website work on wordpress  Now I do dirb for getting open/hidden directories of web server    Here I get hidden directories in website, so now I take a look at hidden directories    Here this message appears to be a note or alert to someone name c0ldd, reminding them that they changed huge’s password and asking them to send it to hugo so he can continue his work  Since the site is built on wordpress I am using wpscan to try and find username’s      As we see I get three username “c0ldd, hugo and Philip”  So now I crack password of this three user’s with wpscan in brute-force mode  When I do brute-force it’s takes lot of time and I get login credentials of “c0ldd” so now I mention c0ldd user only      I get username:- c0ldd password:-9876543210  So now I can login WordPress  Step 3    As you see I can access WordPress now. You notice this WordPress version is outdated so now, so I add reverse shell php and get reverse connection in my terminal    Here the theme edit page ( appearance -> editor -> footer) and then I upload reverse php  ( <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php> )      After upload in footer I add “ip” and “port no” for reverse connection and then update file  Step 4  Now I start my listening    And after this I refresh my main page and then I get my reverse connection in my terminal    For reliable use I add python      I found first flag but I didn’t have permission because I am now data not user. so now I find different way to get access this flag    So I move myself in /var/www/html after that then I find ‘configue.php’    Like this, now I use cat command for reading database    This thing I want, I get username & password of ssh so now I can login ssh with credentials  Step 5    Now I can access user flag now    Here I found my first flag, but the data it’s encoded so now I decode this data in my terminal    After decode I get a message but this one is from another language so now I translated this in google    here the message is ‘ congratulation, first level achieved’  step 6  now I do sudo -l this shows me the allowed and forbidden commands for the current user based on the sudoers configuration.    As you see I get 3 way to gain root access but I show you the easiest one ‘vi’ & ‘ftp’   1. **Becoming Root Via Vi**   First I write a command “sudo /usr/bin/vim”      Then enter after that you are access ‘VI’ first do “shift + colon” then type ‘!sh’ after that you become root    Like this I become root user and obtained my final flag  And for translation I did same like user flag       1. **Becoming Root User Via Ftp**   First I write command like last time then ‘!sh’ and I become root    As you see I become root in 2 easiest way and I complete this machine |
| Reference | https://infosecwriteups.com/colddbox-easy-vulnhub-walkthrough-cac3680e03c2 |

CVE report :- <../coldboxeasy.csv>