|  |  |
| --- | --- |
| Describe | Vulnerability |
| Service | SSH,HTTP |
| Port | 21,80 |
| Versions | 2.4.38 |
| Severity | Medium |
| Cve id | N/A |
| Cvss score | 6/10 |
| Remediation | 1. Avoid Hardcoding Sensitive Information:  Vulnerability: Hardcoding sensitive data, such as encryption keys, in client-side scripts can lead to unauthorized data access.  Remediation: Store sensitive information securely on the server side and ensure it's not exposed to clients.  2. Implement Robust Authentication Mechanisms:  Vulnerability: Weak or easily guessable SSH credentials can be exploited by attackers.  Remediation: Enforce strong password policies and consider using key-based SSH authentication to enhance security.  3. Secure Web Application Endpoints:  Vulnerability: Unprotected endpoints like opus-details.php can be manipulated to access unauthorized data.  Remediation: Implement proper access controls and input validation to ensure that only authorized users can access specific endpoints.  4. Regularly Update and Patch Systems:  Vulnerability: Outdated software can contain known vulnerabilities that are exploitable.  Remediation: Maintain an effective patch management process to ensure all software components are up-to-date with the latest security patches.  5. Conduct Regular Security Audits:  Vulnerability: Unidentified vulnerabilities can persist without regular assessments.  Remediation: Perform regular security audits and code reviews to identify and remediate potential vulnerabilities proactively. |
| POC | Step 1  First we find our ip in arch/kali linux    After this I find target ip with the help of netdiscover    As we see I get target ip now I try to grathering some more information like open ports    After doing Nmap I get open ports SSH and http  http port are open so now i take a look of website    Here a website so now I find open directories with the help of dirb  Step 2    Now I checking one by one all directory for getting some clues    After opeing JS(javascript) directory I get some here    Here some clue as we see at the first one I get clue  ( window.locationnhref = “opus-details.php?id=”+str;)  Here this like I get clue for putting “opus-details.php?id=”+str; line in url  And the second one some details are hidden with the help of AES encryption and I get password for decrypt  Step 3  (SecretPassphaseMovementum) so now first I put that line in url lets see what happen then    In this position website is likely talking the value of the id parameter for the URL (id=ls) and displaying id directly on the page without modification. Now I trying with same step with script tag    Some accursed happen lets try different way      As we see I get cookies wile intercept in inspector mode  This cookies is encrypted so the  (SecretPassphaseMovementum) is the password of encrypted cookies lets check out      Step 4  After decrypt I get one more clue “Auxerre-alienum##”  I this I can login this with SSH  But first I make wordlist of Auxerre-alienum for username and password    As we see here the wordlist of username  same wordlist I use in password also  for password cracking I use ‘hydra’ cmd    After using hydra cmd I get username and password of SSH  Step 5    As you see I get successful login of user    I get user flag easily but now I want to find another user or superuser  But in this position I can’t do anything after some research I get cmd “PS aux”  PS aux= this ps aux command in linux is used to display detailed information about running processes . here’s breckdown of what it’s does    As you see I get lot of running process so now  Now I use “redis-cli” cmd  Redis-cli= the redis-cli command-line tool is used to interact with a redis database. Below are some common commands and use cases.    Like this it’s what I said  After this I use “KEYS \*”  KEYS \*= the command KEYS \* in redis is used to list all keys in the current database.    Like this I said  After that I do ‘get rootpass’    After doing this I get root and root pass  Now I try to access root from this root passsword lets see I get or not    Like that what I expected I become root now  Lets capture root flag    And done!!! |
| Reference | https://www.infosecarticles.com/momentum-1-vulnhub-walkthrough/ |

Csv :- [..\MOVEMENTUM.csv](../MOVEMENTUM.csv)