|  |  |
| --- | --- |
| describe | Vulnerability |
| Service | FTP,SSH |
| Port | 21,22 |
| Versions | 2.4.38 |
| Severity | Medium |
| Cve id | N/A |
| Cvss score | 5/10 |
| Remediations | The **bluemoon:2021** virtual machine on vulnHub is designed for security enthusiasts to practice penetration testing and remediation techniques.   1. **Initial access via ftp credentials:**  * **Vulnerability**: the system exposes FTP credentials through a QR code on its web interface. * Remediation: * ***Secure senstive information:-*** Ensure that sensitive data, such as credentials, are not embedded in publicly accessible areas. * ***Access controls:***- restrict access to sensitive directories and files using proper permissions. * ***Regular audits:***- conduct periodic reviews of web content to identify and remove unintended data exposure.  1. ***Weak password policy for SSH Access:***  * ***Vulnerability:-*** the user ‘robin’ employs a weak password, making the system susceptible to brute-force attacks. * ***Remediations:-*** * ***Enforce strong password policies:-*** Implement requirements for complex passwords, including length and character variety. * ***Account lockout mechanism:***- introduce account lockout policies after a certain number of failed login attempts to failed login attempts to deter brute-force attacks. * ***Multi-factor authentication(MFA):-*** Enhance security by requiring multiple forms of verification for user access.  1. ***Insure Script Excution With Elevated Privileges:-***  * ***Vulnerability:-***  the script /home/robin/project/feedback.sh can be executed with ‘Jerry’ user privilages, and it improperly handles user input, leading to potential command injection. * ***Remediations:-*** * ***Input validation:-*** Sanitize and validate all user input to prevent arbitrary command execution. * ***Principle Of Least Privilege:-*** limit script executions permissions to only those users who absolutely need it. * ***Use Of Secure Coding Practices:-*** Adopt secure coding standards to mitigate vulnerabilities related to script executions.  1. ***Missconfigured Docker Permissions Allowing Privilege Escalations:-***  * ***Vulnerability:-*** the user ‘jerry’ is a part of the ‘docker’ group when necessary, as it grants elevated system access. * ***Remediations:-*** * ***Restrict Group Membership:-*** Only assign users to the ‘docker’ group when necessary, as it grants elevated system access. * ***Monitor And Audit Group Membership:-*** Regularly review Group memberships to ensure compliance with security policies. * ***Educate Users:-*** Inform users about the security implications of being part of privileged groups like ‘docker’. |
| POC | Step 1  At first we find our ip add in kali  After that first we find victim IP add with the help of Netdiscover  ( Netdiscover -r 192.168.1.104/24 )    After that I do Nmap. Nmap works by sending IP packets and analyzing the responses  (Nmap -sT 19.168.1.103)    Step 2  After that we see the interface like this    Now I find directory in this page with the help of ‘gobuster’    After doing gobuster I find a hiden file (/hidden\_text)  Step 3    Here we found a message in that “sorry for the delay. We will recover soon.”  Let’s see in source code I hope some thing I found there  Step 4      As you see I found QR code in source code so I use  ( <https://dnschecker.org/qr-code-scanner.php> )  For reader inside the code    In that code I get user and password for ftp login  User=useftp  Password=ftp@sssword  Step 5  Now I do ftp 192.168.1.103 and put ‘user’ and ‘password’ that I get in QR code      In this I get 2 imp files!  Now I download both of it    Step 6  Lets read both file with ‘cat’ Command    After that I get chat from unknow person to ‘robin’    And the second one I get pass word file  I think robin is user and this one pass file of robin  So now I use hydra for ‘brute force’ attack    After that I get user ‘robin’ and password ‘k4rv3ndh4nh4ck3r’  Step 7    So now I do ssh for login  Ssh robin@192.168.1.103    Lets find the first flag!!    As you see I get first flag  now i see what’s inside in project  after opening project I get other directory but I cant open  Step 8  In new director I get new user ‘jerry’    After that you see I get hint  ‘you reach near to me… try to find me root’  Step 9  In that I found more more thing this this suer base on docker so, I use payload for docker  (Docker -v /:/mnt –rm -it alpine chroot /mnt sh)  After that I get root access after using payload    After that you see I get root access  Now,Let’s find a root flag!!    As you see I found a root flag!! |

Cvs:- [..\bluemoon.csv](../bluemoon.csv)