|  |  |
| --- | --- |
| Describe | Vulnerability |
| Service | http, ssh (raqmon-pdu) |
| Port | 80, 7744 |
| Versions | 4.7.10 |
| Severity | high |
| Cvc I’d | N/A |
| Cvss score | 8/10 |
| remediations | 1. Use of Default or Weak Credentials:  Vulnerability: The application employs default or easily guessable credentials, facilitating unauthorized access.  Remediation:  Enforce Strong Password Policies: Implement requirements for complex passwords, including length and character variety.  Regular Password Audits: Periodically review and update passwords to ensure compliance with security policies.  2. Insecure Configuration of SSH Access:  Vulnerability: SSH is configured on a non-standard port (7744) but allows access with weak credentials, and users are placed in a restricted shell (rbash) that can be easily bypassed.  Remediation:  Implement Strong Authentication Mechanisms: Use complex passwords and consider multi-factor authentication to prevent unauthorized access.  Enhance Shell Restrictions: Ensure that restricted shells cannot be easily bypassed by limiting available commands and removing access to editors like vi that can spawn new shells.  Regularly Update and Patch Systems: Keep SSH and related services up-to-date to protect against known vulnerabilities.  3. Improper Use of Sudo Permissions:  Vulnerability: Certain binaries, such as git, are allowed to run with elevated privileges without proper restrictions, enabling privilege escalation.  Remediation:  Restrict Sudo Access: Limit sudo permissions to only those commands necessary for specific users, and avoid granting unrestricted access to powerful binaries like git.  Regular Audits: Conduct periodic reviews of the /etc/sudoers file to ensure compliance with the principle of least privilege. |
| POC | Step 1  First,I find our ip in kali linux    Then I find dc-2 ip from netdiscover    Then I do nmap for checking open port of DC-2    Step 2  Port no 80 are open (http) now I going to see dc-2 website for more informations      Firewall didn’t know about dc-2 lets add it from nano  (nano etc/hosts)      Let’s see again website    Step 3  I get flag 1 from website, now he trying to tell us for doing crewl (crewl cmd help for creating password from website!!)    Now I do crewl cmd for making password and saving directly by “>” this command    Now I do WPS scan for getting sensitive information about website (like theme,users,version)      As you see I get 2 users tom and jerry  Now I make file with the help of nano    Like this  Now I do brute-fore attack with the help of wpscan      Like this I got password of tom and jerry  Step 4  Now I do login tom from ssh (7744 Raqmon-pdu)      I get flag3.txt but I can’t access because of -rbash  Now I find path with the help of “echo” cmd    Now I use ‘VI’ for removing rbash    :Set shell=/bin/bash  :shell  And then rbash will be remove from path  Step 5  Now I try to see ‘flag3.txt’    bash cmd also remove while removing rbash so I use echo $(<flag3.txt) for looking flag3  here we get another hint for accessing ‘jerry’ user  but first I want to export bash    With the help of this command bash added to my terminal    Now here I can’t find jerry now I move to another directory    From another directory I can access jerry user now I try to access root from jerry  Step 6    In this place I can’t do anything, I can’t access any single directory    Now I do sudo -l do  This command lists the sudo privileges of the current users. It shows what commands the users is allowed to run with sudo and whether a password is required  And the below i get another hint root have no password so I can access easily    In this position I didn’t have permission to access root  So I do git help cmd for using cmd normally      After importing (!/bin/bash) in (sudo git help add) now I get root    Like this  After this now I try to get super-user    Now I get super-user as you see |
| References | https://medium.com/@t0thkr1s/dc-2-walkthrough-37e374217df1 |

Csv :- [..\DC-2.csv](../DC-2.csv)