|  |  |
| --- | --- |
| Machine Description | Photographer is a boot2root web exploitation lab where an attacker abuses insecure image management and hidden admin functionality. The machine teaches web file handling abuse, privilege escalation, and full system compromise scenarios. |
| Target IP | 10.84.42.93 |
| Vulnerability Name | Unauthenticated remote code execution (RCE) through admin file handling |
| Port / Service | TCP 445 / SMB  TCP 8000 / HTTP |
| CVSS Score and severity | 9.8 Critical |
| Attack Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| Proof Of Concept | STEP 1 – Discover the target machine IP using Netdiscover    STEP 2 – Look For Open ports and Services running on the target system using Nmap    STEP 3 – Lets Enumerate findings and gather information about target   1. Visiting Web page hosted on server to gather information      1. Lets look for the files on the web server port 80      1. Lets now look for the directories on server port 80      1. Lets look for files on port 8000      1. Lets look for directories on port 8000      1. We have /admin panel on 8000 a CMS login KOKEN     We Found that during the Nmap scan target is running the SMB so lets try to enumerate and find what we get there  STEP 4 – Lets try Enum4Linux on SMB port 445 and lets see is there any null session possible    STEP 5 – As we can see Null Sessions is allowed so lets try to find manually that we can find any shared folders     1. We got Null session and found share folder named sambashare 2. We also found two files on share server lets enumerate them      * Valid User 1 Daisa Ahomi daisa@photographer.com * Valid User 2 Agi Clarence agi@photographer.com * Secret : babygirl for Daisa   STEP 5 – Lets Try to use these content on CMS    And we got Login, So lets look for the upload functionality and try to upload because we found about CMS in exploit DB we got file upload relevant thing         * So lets try out as mention in the exploit first lets create exploit from pentest monkey and save as image.php.jpg        * Open burpsuite an try to upload the file trying to bypass file upload restriction and uploading our shell      * Setup netcat listner        * We will trigger the shell by integrating with options      * We can see we got Shell on target System     STEP 6 – Now lets look for privilege escalation we have php7.2  We can look for GTFOBiins and try go get root access       * Also update password for the users |
| Impact | * high confidence of remote shell and system takeover. * sensitive files and credentials can be exfiltrated. * attack can be used to pivot to other hosts. * integrity and availability of services can be fully lost. |
| Remediations | * remove or restrict public access to admin interfaces. * validate and sanitize all uploaded filenames and input. * apply least privilege for web processes and enable chroot or containers. * deploy WAF, apply host hardening, and monitor for indicators of compromise. |
| Reference | <https://www.exploit-db.com/exploits/48706>  <https://vulners.com/exploitdb/EDB-ID:48706>  <https://lifesfun101.github.io/2020/08/09/Photographer-walkthrough.html> |