|  |  |
| --- | --- |
| Describe | Vulnerability |
| Service | HTTP |
| Port | 80 |
| versions | 2.2.22 |
| Severity | Medium |
| CVC id | N/A |
| CVSS SCORE | 7/10 |
| Remediations | **Common Vulnerabilities in DC:1:**   * **Drupalgeddon 2 (CVE-2018-7600)** – A critical remote code execution flaw in Drupal. * **Outdated software versions** – Drupal, Apache, PHP, etc. * **Misconfigured web services** – Directory listing, default credentials, etc.   **Remediation Steps:**   1. **Update Drupal CMS**    * Ensure the Drupal version is **at least 7.58+ or 8.5.1+**, which fixes CVE-2018-7600.    * Always run the latest supported version of Drupal. 2. **Harden PHP Configuration**    * Disable functions like exec, passthru, and shell\_exec.    * Set appropriate file permissions. 3. **Secure Apache Configuration**    * Disable directory listing (Options -Indexes).    * Remove unnecessary modules.    * Enable security headers like Content-Security-Policy, X-Frame-Options, etc. 4. **User Management**    * Remove or rename default accounts.    * Enforce strong passwords and multi-factor authentication (MFA). 5. **Firewall & Intrusion Detection**    * Use a firewall to restrict access to essential services.    * Deploy tools like Fail2Ban or OSSEC to monitor for brute-force or exploit attempts. 6. **System Updates**    * Regularly update the OS and software dependencies. 7. **Backup & Recovery**    * Implement regular backups with secure offsite storage.    * Test recovery procedures. |
| poc | Step 1 :-  First i find our ip    After that i find target ip    i get target ip add (192.168.1.106)  now i find open ports of target    i get 3 open ports now I see port 80(http) about target    Step 3:-  As you see port 80 open now I find vulnerability about Drupal in Metasploit    I choose API property injection for attack    I set rhost for attack    As you see I get meterpreter I giving command shell and I get  Step 4:-  After that I ask which python    After this then I giving python payload    python -c 'import pty; pty.spawn("/bin/bash")'  python -c: Runs the given Python code as a command.  import pty: Imports Python's pseudo-terminal module.  pty.spawn("/bin/bash"): Spawns a new interactive bash shell through the pseudo-terminal.  After that I become user as you see  After this I giving one more payload for getting root directly    Find / -perm -u=s -type f 2>/dev/null  find /: Searches the entire filesystem starting at the root directory (/).  -perm -u=s: Looks for files with the SUID permission bit set (u+s)  -type f: Limits the search to regular files (ignores directories, sockets, etc.).  2>/dev/null: Suppresses error messages (e.g., "Permission denied").  Step 5:-  After that I move myself in temp file and create now folder for one last payload    Find (file name) -exec “/bin/sh” \; after executing this I get root access  File name (Reaper): with the file name you are looking for.  -exec: Runs a command on each file found by find.  /bin/sh: Executes /bin/sh on the file found  Step 6:- I found root as you see!!!    For more information you can see from here |
| References | https://medium.com/@surajtech72/dc-1-vulnhub-walkthrough-b8e69030178a |

Csv :- [..\DC-1.csv](../DC-1.csv)