SAFE SECURITY

Ubuntu OverlayFS Local Privesc Vulnerability

CVE-2021-3493

Rohit Verma, Sudhanshu Kumar

SAFE SECURITY

Table of Contents

CVE-2021-3493 is an Ubuntu-specific issue in the overlayfs file system in the Linux kernel where it did not properly validate the application of file system capabilities to user namespaces. A local attacker could use this to gain elevated privileges, due to a patch carried in Ubuntu to allow unprivileged overlayfs mounts.

Keywords: OverlayFS, Mount, Union Mount, File capabilities

Introduction

This Document illustrates the Exploitation of the vulnerability found in Ubuntu in which the OverlayFS file system allows local users under Ubuntu to gain root privileges. The Vulnerability was reported by an independent security researcher to the SSD Secure Disclosure program and was allotted CVE on 04/17/2021.

OverlayFS

OverlayFS is a union mount filesystem on Linux. It is a Linux kernel module that allows the system to combine several mount points into one so that you can access all the files from each within one directory structure.
It is often used by live USBs or some other specialist applications. One use is having a read-only root file system and another partition overlayed with that to allow applications to write a temporary file system.

Mount

Mount is a process by which the operating system makes files and directories on a storage device (such as hard drive, CD-ROM, or network share) available for users to access via the computer's file system.

Union Mount

Union Mount is a way of combining multiple directories into one that appears to contain their combined contents.

File capabilities

File Capabilities aims to provide fine-grained control over root permissions. These capabilities are a partitioning of all root privileges into a set of distinct and independent privileges. Using these functionalities, reduces/prevents the need to switch as the root user.

Exploit Working

The exploit is done by executing a C file on the machine. If the system is vulnerable, you can escalate very easily from any user to root as long as you can run a binary.
The exploit used requires a GCC compiler installed on the system if there is not a C compiler installed on the machine, you can compile the binary statically elsewhere and copy just the binary over.

CVSSv3:

- Base Score – 7.8
- Impact Score - 5.9
- Exploitability Score - 1.8
- Severity - HIGH

Scope Impact:

The scope of this vulnerability is that the attacker can have access to all commands and files on a vulnerable machine.

.

Affected Versions	Unaffected Versions
Ubuntu 20.10	Another distribution of Linux is not affected because this issue is likely Ubuntu-specific, as Ubuntu carries a patch to enable unprivileged overlayfs mounts.
Ubuntu 20.04 LTS	
Ubuntu 18.04 LTS	
Ubuntu 16.04 LTS	
Ubuntu 14.04 ESM	

Mitigation:

A commit that addresses the issue was applied in the upstream kernel:

7c03e2cda4a5 ("vfs: move cap_convert_nscap () call into vfs_setxattr ()") (v5.10)

It was added prior to the upstream kernel commit allowing unprivileged overlayfs mounts:

459c7c565ac3 ("ovl: unprivileged mounts") (v5.11)

The problem can be corrected by updating your kernel live patch to the following versions:

Ubuntu 20.04 LTS
AWS - 76.3
azure - 76.3
gcp - 76.3
generic - 76.3
gke - 76.3
gkeop - 76.3
low latency - 76.3

Ubuntu 16.04 LTS
aws - 76.1
azure - 76.2
generic - 76.2
lowlatency - 76.2

Ubuntu 18.04 LTS
aws - 76.2
generic - 76.3
gke - 76.3
gkeop - 76.3
lowlatency - 76.3
oem - 76.2

Ubuntu 14.04 ESM
generic - 76.1
lowlatency - 76.1

Kernels older than the levels listed below do not receive live patch updates. If you are running a kernel version earlier than the one listed below, please upgrade your kernel as soon as possible.

Ubuntu 16.04 LTS
linux-aws - 4.4.0-1098
linux-azure - 4.15.0-1063
linux-azure - 4.15.0-1078
linux-hwe - 4.15.0-69
linux - 4.4.0-168

Ubuntu 20.04 LTS
linux-aws - 5.4.0-1009
linux-azure - 5.4.0-1010
linux-gcp - 5.4.0-1009
linux-gke - 5.4.0-1033
linux-gkeop - 5.4.0-1009
linux-oem - 5.4.0-26
linux - 5.4.0-26

Ubuntu 18.04 LTS
linux-aws - 4.15.0-1054
linux-gke-4.15 - 4.15.0-1076
linux-gke-5.4 - 5.4.0-1009
linux-gkeop-5.4 - 5.4.0-1007
linux-hwe-5.4 - 5.4.0-26
linux-oem - 4.15.0-1063
linux - 4.15.0-69

Ubuntu 14.04 ESM
linux-lts-xenial - 4.4.0-168

Lab Setup

1. Ubuntu Machine (Affected Version)
2. Git tools (To clone repository)
3. GCC Compiler (To compile c file)

Exploit Implementation

1. Use the command whoami and id to check the privilege of the current user.

   Command: whoami

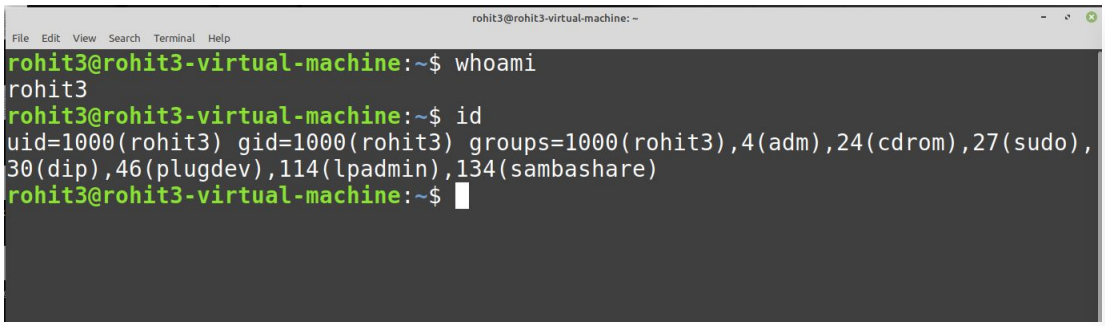

Fig. 1.1

2. To get the exploit - Clone the repository using the below command.
   Ensure that git is installed in your system. If not installed use the below

   Command: sudo apt-get install git

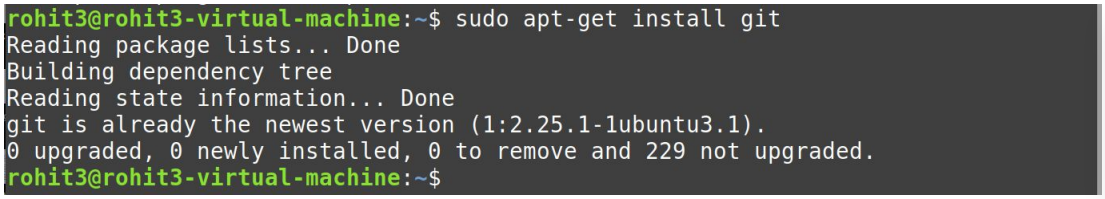

Fig. 2.1

   Once the git is installed clone the repository using the following command.

   Command: git clone https://github.com/briskets/CVE-2021-3493.git

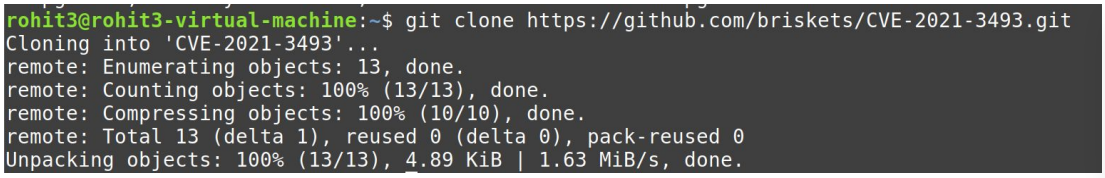

Fig. 2.2

Exploit Implementation

3. After cloning the new file named CVE-2021-3493 is created in the present directory, navigate to that directory by using the

Command: cd CVE-2021-3493
After that list the files in the directory using the

Command: ls

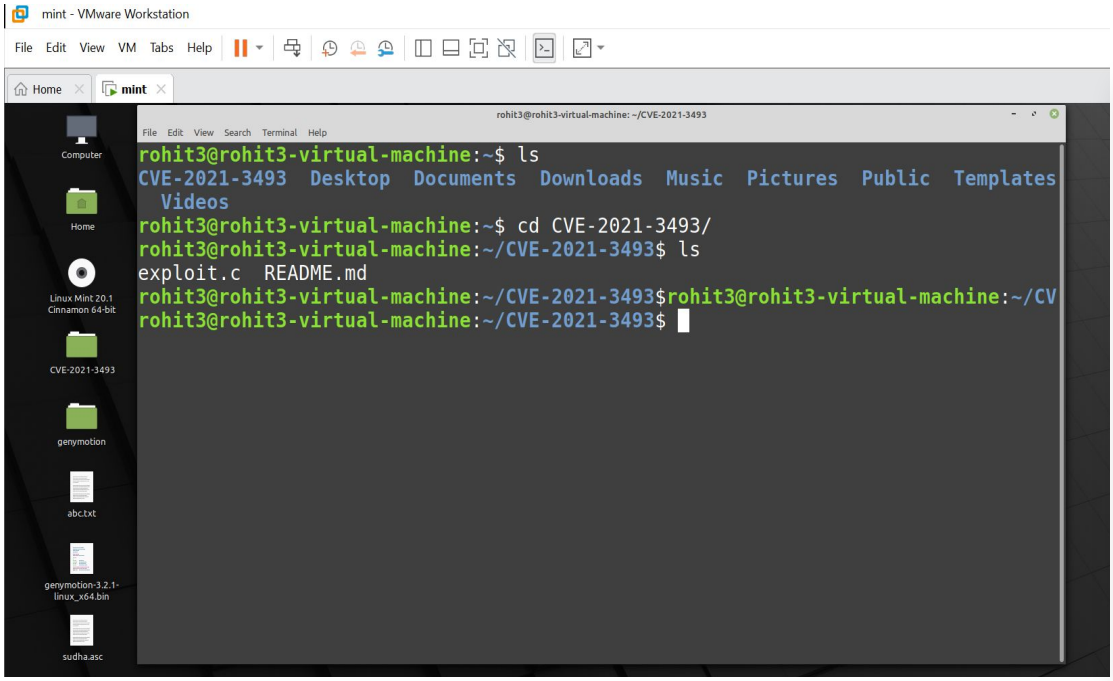

Fig. 3.1

4. There is a file named exploit. c which is the c file. So, compiling it using GCC compiler.

Command: gcc exploit.c

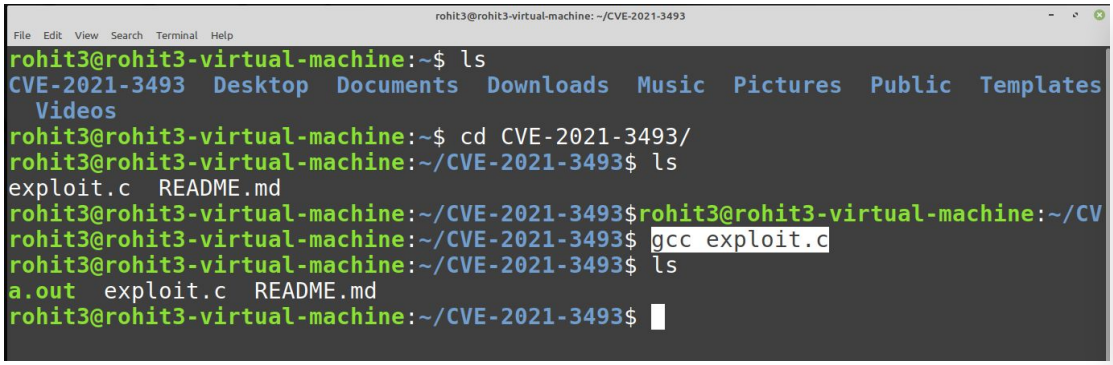

Fig. 4.1

Exploit Implementation

5. If you do not provide any output file name by default a.out will be created.

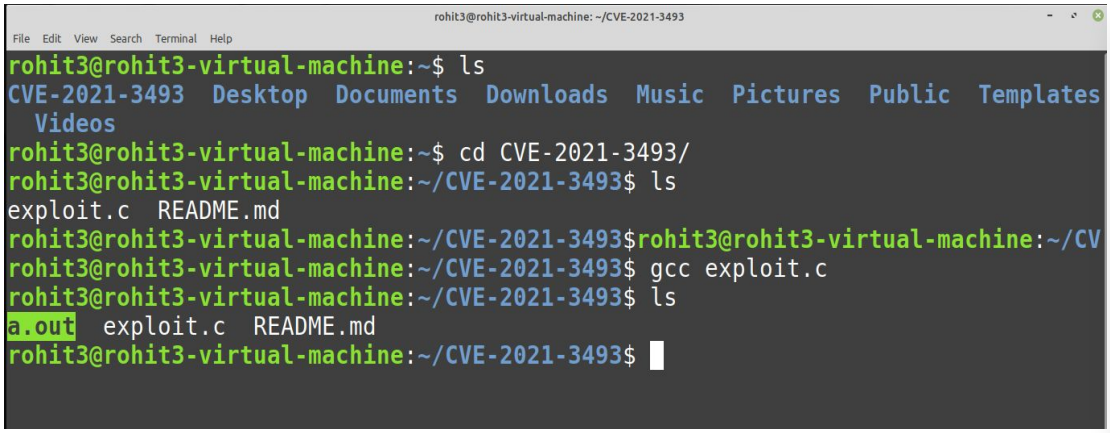

Fig. 5.1

6. Execute the exploit using the below

Command: ./a.out

After executing a new shell will be created and verify the privilege using

Command: whoami and id.

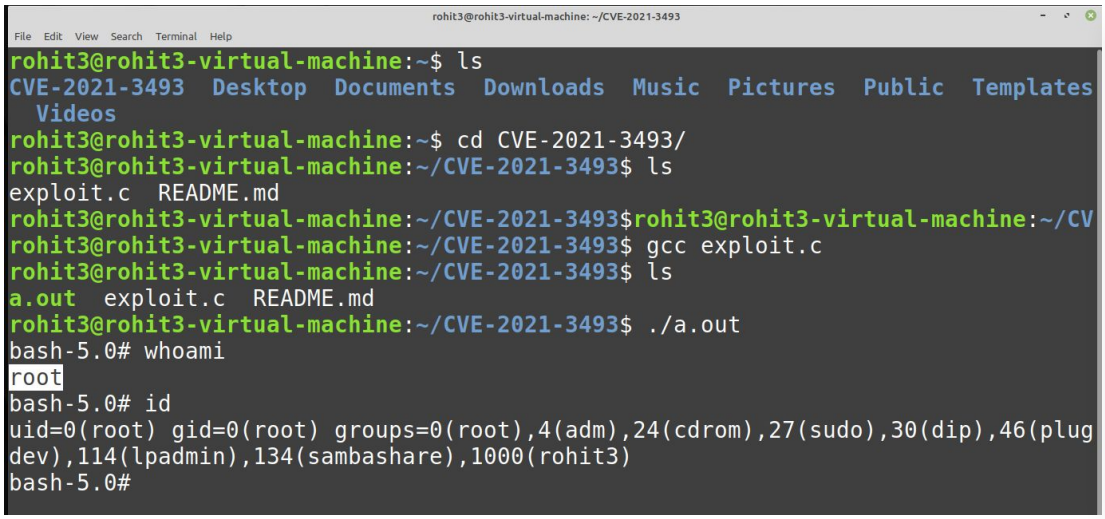

Fig. 6.1

Exploit Implementation

7. Now we have gained the Privilege of the root user.

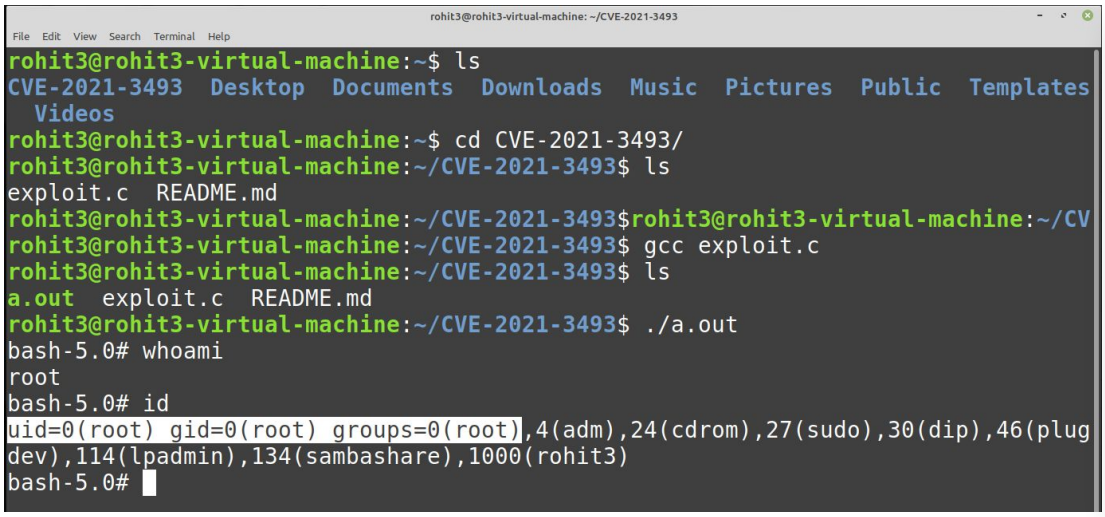

Fig. 7.1

8. Now with root privileges you have access to all commands and files on a Linux machine. Attackers can now add, delete users or change their password or do anything that they want to do.

Initially, we were not able to change the password of user1 but after running the exploit you gain the access to the root user and now you can change the password of user1.

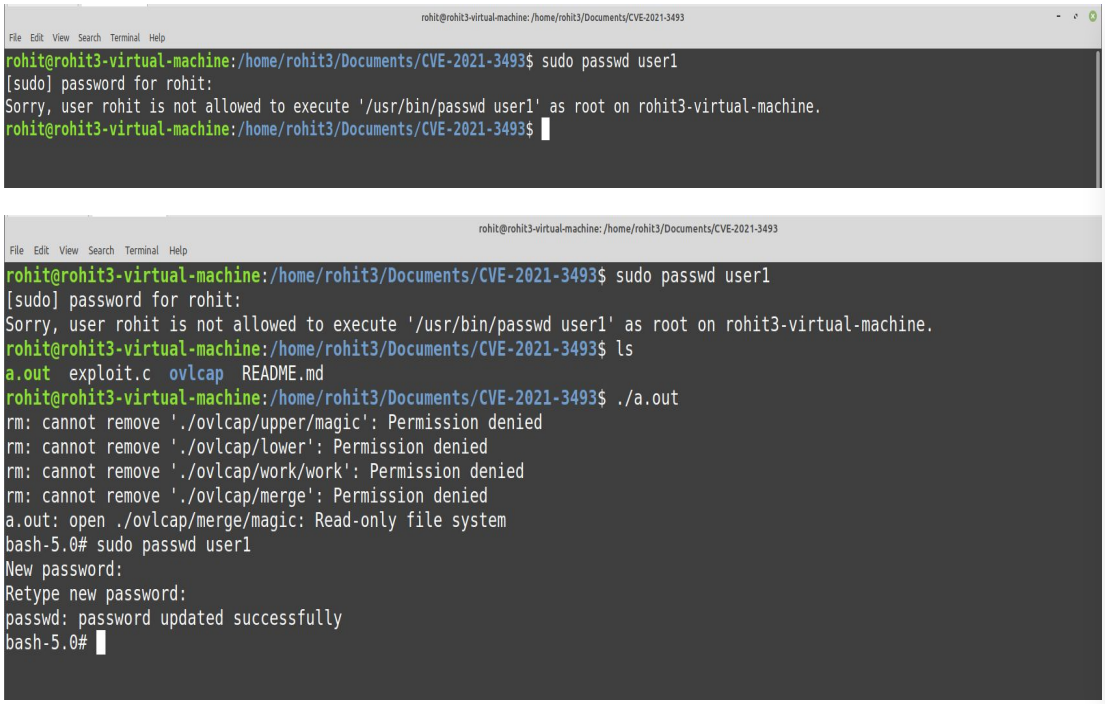

Fig. 8.1

References

- https://github.com/briskets/CVE-2021-3493
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3493
- https://nvd.nist.gov/vuln/detail/CVE-2021-3493
- https://ssd-disclosure.com/ssd-advisory-overlayfs-pe/

www.safe.security | info@safe.security

Standford Research Park,
3260 Hillview Avenue,
Palo Alto, CA - 94304