

Linux Kernel – Local Privilege Escalation - CVE- 2018-18955



R. A. SHEHAN SANJULA

IT19154404

GROUP 13.1

IE2012 – SYSTEMS AND NETWORK PROGRAMMING



Table of Contents



1) Introduction.....	3
2) Vulnerability Discovery Details	5
3) Screenshots of the Exploitation	9
4) Conclusion	10
5) References	11



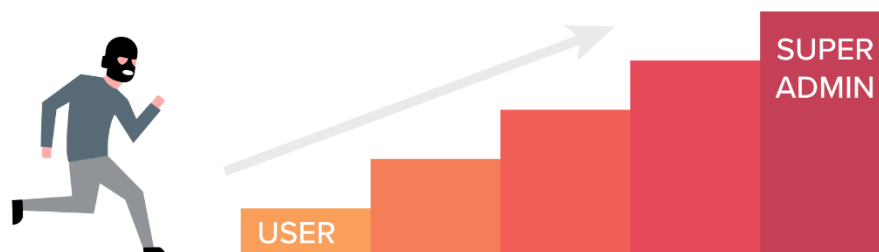
1. Introduction



➤ What is Privilege Escalation?

Privilege escalation happens when a malicious user exploits a bug, design flaw, or configuration error in an application or operating system to gain elevated access to resources that should normally be unavailable to that user. The attacker can then use the newly gained privileges to steal confidential data, run administrative commands or deploy malware – and potentially do serious damage to your operating system, server applications, organization, and reputation.

PRIVILEGE ESCALATION



➤ **How does privilege escalation work?**

Attackers start by exploiting a privilege escalation vulnerability in a target system or application, which lets them override the limitations of the current user account.

However, if you can quickly detect successfully or attempted privilege escalation, you have a good chance of stopping an attack before the intruders can establish a foothold to launch their main attack.

➤ **Why privilege escalation is important?**

While usually not the main aim of an attacker, privilege escalation is frequently used in preparation for a more specific attack, allowing intruders to deploy a malicious payload or execute malicious code in the targeted system. This means that whenever you detect or suspect privilege escalation, you also need to look for signs of other malicious activity.



2. Vulnerability Discovery Details



- ✓ So, in this report, I am going to review vulnerability called privilege escalation of the Linux kernel environment. (CVE 2018 - 18955)
- ✓ **Jann Horn** discovered that the Linux kernel mishandles mapping UID or GID ranges inside nested user namespaces in some situations. This vulnerability was found in **2018**. A local attacker could use this to bypass access controls on resources outside the namespace.
- ✓ In the Linux kernel 4.15.x through 4.19.x before 4.19.2, `map_write()` in `kernel/user_namespace.c` allows privilege escalation because it mishandles nested user namespaces with more than 5 UID or GID ranges. A user who has `CAP_SYS_ADMIN` in an affected user namespace can bypass access controls on resources outside the namespace, as demonstrated by reading `/etc/shadow`.

- ✓ This occurs because an ID transformation takes place properly for the namespaced-to-kernel direction but not for the kernel-to-namespaced direction.

➤ Common Vulnerability Scoring System (CVSS) Score Details

CVSS v3 Score Breakdown - NIST and Red Hat

	Red Hat	NVD
CVSS v3 Base Score	7.8	7.0
Attack Vector	Local	Local
Attack Complexity	High	High
Privileges Required	Low	Low
User Interaction	None	None
Scope	Changed	Unchanged
Confidentiality	High	High
Integrity Impact	High	High
Availability Impact	High	High

➤ Exploitation technique used: *ld.so.preload* Technique.

- ✓ In this exploitation, I am going to discuss a new technique of privilege escalation by exploiting an environment variable "LD_Preload".

Shared Libraries

- ✓ Shared libraries are libraries that are loaded by programs when they start. When a shared library is installed properly, all programs that start afterwards automatically use the new shared library.

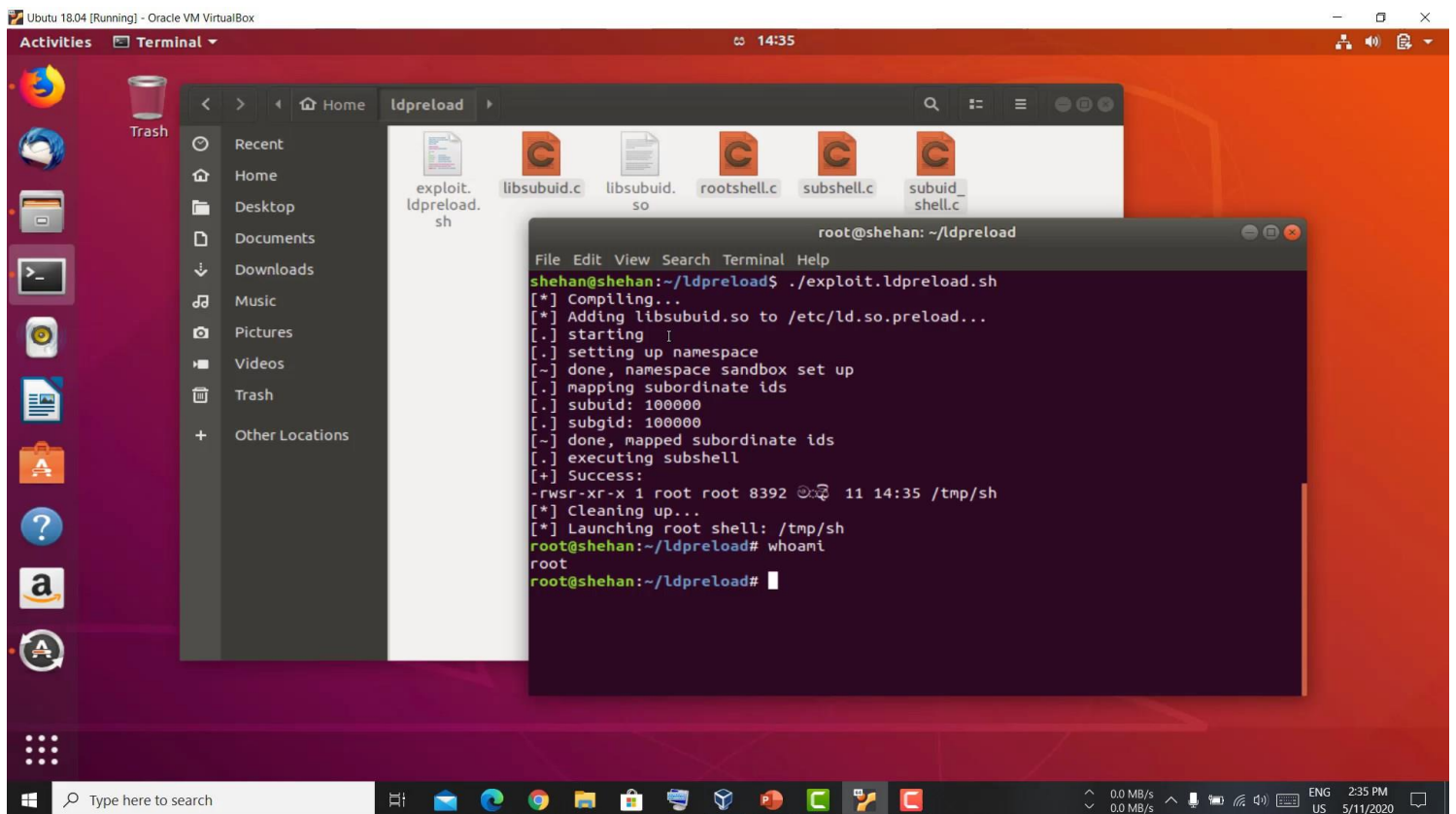
Shared Libraries Names

- ✓ Every shared library has a special name called the "**soname**". The soname has the prefix "**lib**", the name of the library, the phrase "**.so**", followed by a period and a version number.
- ✓ The dynamic linker can be run either indirectly by running some dynamically linked program or shared object. The programs **ld.so** and **ld-linux.so*** find and load the shared objects (shared libraries) needed by a program, prepare the program to run, and then run it.

- ✓ **LD_Preload**: It is an environment variable that lists shared libraries with functions that override the standard set, just as **/etc/ld.so.preload** does. These are implemented by the loader **/lib/ld-linux.so**



3. Screenshots of the Exploitation



The screenshot displays a Linux desktop environment (Ubuntu 18.04) running in an Oracle VM VirtualBox. A file manager window is open, showing the contents of the `ldpreload` directory. The files listed are `exploit.ldpreload.sh`, `libsubuid.c`, `libsubuid.so`, `rootshell.c`, `subshell.c`, and `subuid_shell.c`. A terminal window is also open, showing the execution of the `exploit.ldpreload.sh` script. The terminal output indicates that the script is compiling, adding `libsubuid.so` to `/etc/ld.so.preload`, and setting up a namespace. It then maps subordinate IDs, sets up a subshell, and successfully launches a root shell. The user `shehan` is shown as `root` after running `whoami`.

```
shehan@shehan:~/ldpreload$ ./exploit.ldpreload.sh
[*] Compiling...
[*] Adding libsubuid.so to /etc/ld.so.preload...
[.] starting [
[.] setting up namespace
[~] done, namespace sandbox set up
[.] mapping subordinate ids
[.] subuid: 100000
[.] subgid: 100000
[~] done, mapped subordinate ids
[.] executing subshell
[+] Success:
-rwsr-xr-x 1 root root 8392 11 14:35 /tmp/sh
[*] Cleaning up...
[*] Launching root shell: /tmp/sh
root@shehan:~/ldpreload# whoami
root
root@shehan:~/ldpreload#
```



4. Conclusion



- ✓ Attackers can use many privilege escalation techniques to achieve their goals. But to attempt privilege escalation in the first place, they usually need to gain access to a less privileged user account.

➤ **How to Protect Your Systems from Privilege Escalation**

- ❖ Enforce password policies.
- ❖ Create specialized users and groups with minimum necessary privileges and file access.
- ❖ Avoid common programming errors in your applications.
- ❖ Secure your databases and sanitize user input.
- ❖ Keep your systems and applications patched and updated.
- ❖ Ensure correct permissions for all files and directories.
- ❖ Close unnecessary ports and remove unused user accounts.
- ❖ Change default credentials on all devices, including routers and printers.



5. References



- NATIONAL VULNERABILITY DATABASE, NIST. 2020. Accessed: May. 10, 2020 [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2018-18955#vulnCurrentDescriptionTitle>
- Exploit database. Accessed: May. 10, 2020 [Online]. Available: <https://www.exploit-db.com/exploits/47166>
- Hacking Tutorials. Accessed: May. 10, 2020 [Online]. Available: https://www.hackingarticles.in/linux-privilege-escalation-using-ld_preload/
- Mitre. 2020. CVE-2018-18955 Accessed: May. 11, 2020 [Online]. Available <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18955>
- Netsparker Blog 2020. Privilege Escalation Accessed: May. 11, 2020 [Online]. Available: <https://www.netsparker.com/blog/web-security/privilege-escalation/>
- Red Hat 2020. CVE-2018-18955 Accessed: May. 11, 2020 [Online]. Available: <https://access.redhat.com/security/cve/cve-2018-18955>