

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

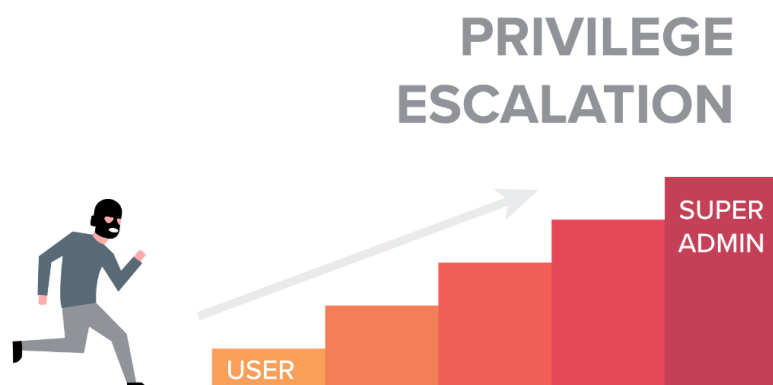


1. Introduction



➤ What is Privilege Escalation?

We can describe privileged escalation when a malicious user exploits the operating system or the application using a bug or a configuration error to obtain restricted access to the system resources which should usually be unavailable to that user. Then, the attacker applies the newly obtained privileges to steal confidential data, run administrative commands or deploy malware. Of course, he or she can do serious damage to our operating system, server applications, organization, and reputation.



➤ **How does privilege escalation work?**

Cyber Attackers try to start exploitation by using this privilege escalation vulnerability in a target system or application. This procedure grants them to override the boundaries of the typical user account.

Hence, if you need to stop an attack before the intruders established an attack, you need to detect successfully attempted privilege escalation quickly.

➤ **Why privilege escalation is important?**

Sometimes the privilege escalation may not be the main target of attackers which they are trying to do. They use this privilege escalation often in preparation for a more specific attack that empowers them to execute a malicious payload or malicious code in the targeted system.

Therefore, you also need to look for hints of other malicious activity whenever you identify or suspect privilege escalation.



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.
- ✓ According to NIST, “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

- ✓ According to the Netsparker, "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

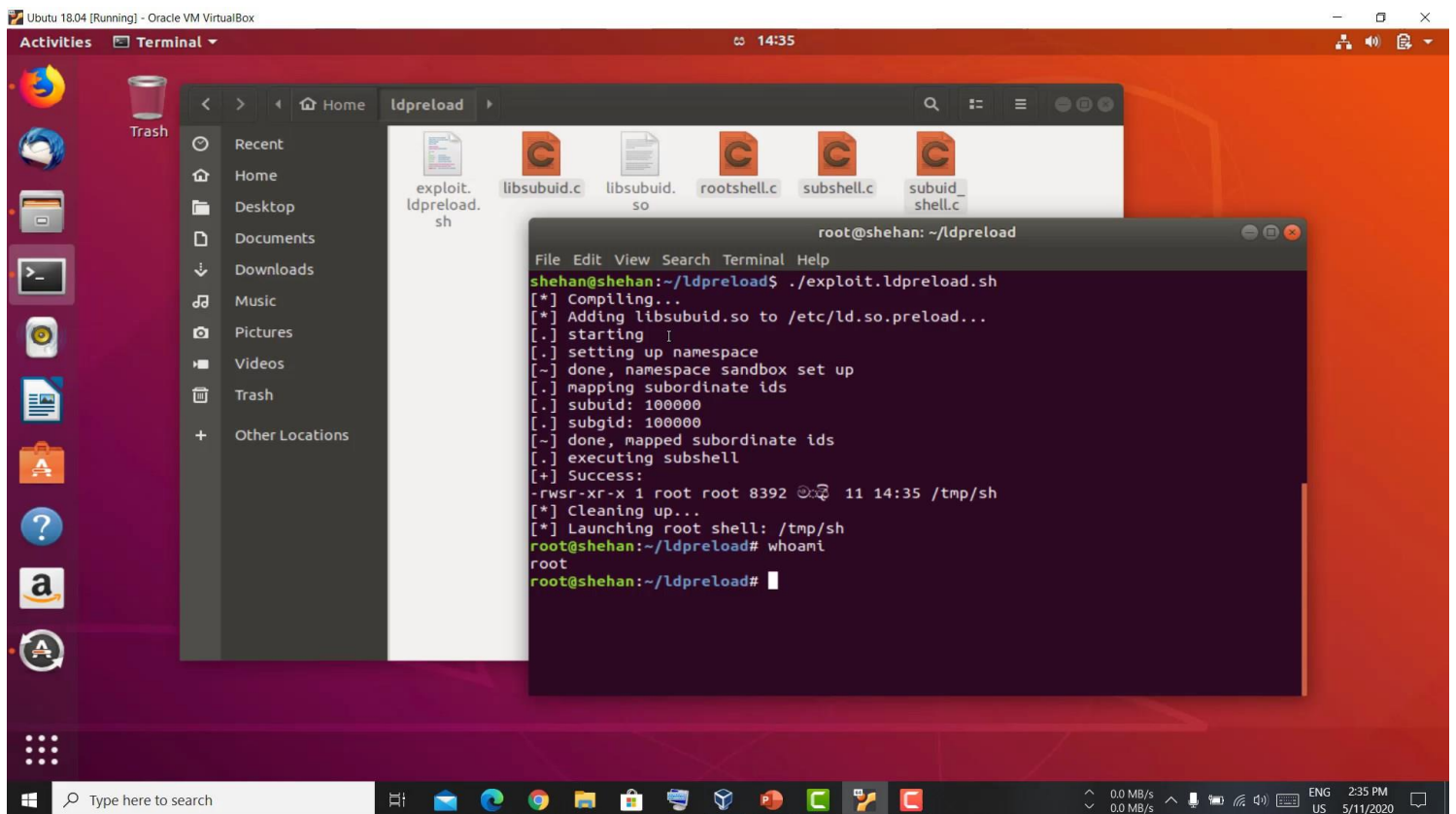
- ✓ Hacking tutorials website describes it as "Every shared library has a special name called the "**soname**". The soname has the prefix "**lib**", the name of the library, the phrase ".so", followed by a period and a version number.
- ✓ The dynamic linker can be run either indirectly by running some 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



```
root@shehan: ~/ldpreload
File Edit View Search Terminal Help
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 multiple privilege escalation techniques to achieve their intentions. Further, they ordinarily need to get access to a less privileged user account before attempt a privilege escalation. The cyber specialists suggest the following practices to protect your systems from privilege escalation.

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

- ❖ Enforce password policies.
- ❖ Create specialized users and groups with minimum necessary privileges and file access.
- ❖ 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>