Sri Lanka Institute of Information Technology

Sudo Vulnerability Exploit CVE-2019-14287

Individual Assignment

IE2012 – Systems and Network Programming

S.A.D. Hasintha Vishwajith
IT19952376

Content

1. Introduction

Sudo has been discovered to be unreliable, one of the most significant, powerful, and commonly used utilities installed in almost any Unix and Linux based operating system as a simple command. A pseudo security policy bypass flaw that allows arbitrary commands to be executed on a targeted Linux device by a malicious user or application. There must be a non-standard setup for the mistake. Linux machines, in other words, are not corrupted by nature. Incorrect users should only use the "Super User Do" command while executing commands on a Linux operating system by defining the user ID "-1" to execute it as a command source [1]. Insecurity needs a structured setup as demonstrated in CVE-2019-14287 but also opens the door to unauthorized users. Using -u # -1 on the command line helps users to circumvent the faux error-caused offline cap.

2. What is Sudo

I. Introduction

There are two ways to incorporate Linux administrative software. With the su button, you can turn to a super user (root) or you can take advantage of Sudo. If you do this relies on the delivery that you are using. The root user is supported by some distributions and some don't. Every has pros and cons. "Substitute User" or "Mega User" means Sudo. In most Linux distributions, what Sudo does is incredibly important and critical. Sudo enables a user to execute a program as another user, efficiently, Ud [3]. There are many people who claim that the only way to get the "best training safe" in Linux is by Sudo. There are some, though, that sound entirely different. There will come a moment when you need to take advantage of Sudo, regardless of where you are, and what distribution you are actually using. If you just want to use Sudo or you would customize Sudo, you may need to know the inside and outside of this important method [2].

II. History of Sudo

Sudo traced the origins of the Department of Computer Science in 1980 to Sunee / Buffalo (created by Bob Kogshal and Cliff Spencer). After its release (adding new functions and changing developers), Sudo has repeated itself over and over again. "At one point, around 1994, Todd Miller of the University of Colorado at Boulder in CO developed the Sudo, and the unofficial" fork "Sudo was released as" CU Sudo. Help for more bug patches and distributions was also introduced by this "fork." This "CU" prefix was finally dropped in 1999, and the Sudo version that we use today is "CU Sudo". Since 1991, the original nickname has not been written. So, "Fork" has prevailed, and it is still being improved by Todd Miller [1].

3. How to exploit

Sudo 1.8.28 Today, October 14, 2019, is the resolution of the following security-related issue assigned to CVE-2019-14287. Potential Bypass Runas User Restrictions Summary: The user can execute the root command by entering "ID-1" or "4294967225" while Sudo is configured to enable the user to execute commands across all keywords as an arbitrary user. This can be used by a person with sufficient Sudo privileges to execute root commands [4]. Both keywords are specified first in the Runas specification. Logs for commands executed in this way will list the target user as "4294967295" instead of "root." Additionally, the PAM session modules are not available for this command.

- Sudo versions prior to 1.8.28 are affected.
- This Sudo vulnerability was assigned "CVE-2019-14287" in the Common Vulnerabilities.

➢ Exploitation Method

Sudo allows the implementation of commands with such a user-specific username or username, as permitted by the pseudo rule. For instance, the below Sudo permission allows every user to run the Id instruction.

```
myhost user = (ALL) /usr/bin/id
```

The "user" user was able to execute the ID command like any legitimate user that could use the" # uid "notation to execute it as an arbitrary user ID.

```
sudo -u#1234 id -u
```

however, Setresuid and setreuid device calls, that use sudo for user ID-1 to change the user ID before the command is executed, do not modify the user ID for this value in particular.

```
sudo -u#-1 id -u
```

Next, If the entry for sudo is written to allow the user to execute the command like any other user other than root, the error can be used to escape this restriction. For instance, the following access is provided to sudo:

```
myhost anne = (ALL, !root) /usr/bin/vi
```

Root, but user Anne is allowed to run vi as root as any user. Because of the mistake, however, Anne can actually run as vi root by running "sudo -u # -1 vi" in a security policy breach. All of the keywords in the Runas specification refer only to entries for sudoers.

```
myhost user = /usr/bin/id
```

In this case, only the I d command can be run as the basis by the user. Any attempt to execute orders from another user will be denied.

4. Conclusion

Sudo CVE-2019-14287 Danger allows for local exploitation by malicious users of such pseudo setups. A special binary from the Linux operating system is Sudo or Super User Do. It is grounded and has some unique permissions. It is known as Setuid. The permissions of the binary owner are immediately inherited by any user who triggers a binary with processing permissions.

5. References

[1] J. W. -, By, -, and J. Wallen, “Linux 101: Introduction to sudo,” Linux.com, 12-May-2010. [Online]. Available: https://www.linux.com/training-tutorials/linux-101-introduction-sudo/.

[2] M. Katchinskiy, “CVE-2019-14287 sudo Vulnerability Allows Bypass of User Restrictions,” Container, Serverless & Cloud Native Application Security, 27-Aug-2020. [Online]. Available: https://blog.aquasec.com/cve-2019-14287-sudo-linux-vulnerability.

[3] “The Top 10 Linux Kernel Vulnerabilities You Should Know.” [Online]. Available: https://resources.whitesourcesoftware.com/blog-whitesource/top-10-linux-kernel-vulnerabilities.

[4] “Find and fix CVE-2019-14287 sudo vulnerability | Puppet.” [Online]. Available: https://puppet.com/blog/find-and-fix-cve-2019-14287-sudo-vulnerability/.