Linux ‘Copy Fail’ Vulnerability Grants Root Access on Major Distros

Description

Cybersecurity researchers have revealed a significant vulnerability in the Linux operating system, enabling a local user without privileges to gain root access. This flaw, identified as CVE-2026-31431 and rated with a severity score of 7.8, has been codenamed "Copy Fail" by firms Xint.io and Theori.

The vulnerability arises from a logical error in the Linux kernel's cryptographic subsystem, specifically within the algif_aead module, which was introduced in a code update in August 2017. This breach permits an unprivileged user to manipulate the page cache of any readable file on a Linux system, effectively allowing them to escalate their privileges to that of a root user.

Exploiting this vulnerability does not require extensive technical knowledge. A simple 732-byte Python script can edit a setuid binary—files that allow users to execute programs with the permissions of the file owner. The exploit follows a series of steps, including opening an AF_ALG socket, constructing a payload, writing to the kernel's cached copy of "/usr/bin/su," and executing it to gain root access.

Though the flaw cannot be exploited remotely on its own, a local user can corrupt the page cache of a setuid binary to escalate privileges. This issue poses additional risks as the affected page cache is shared across processes, potentially impacting containerised environments.

In reaction to the discovery, various Linux distributions have issued advisories regarding the vulnerability. Comparisons have been drawn to a previous exploit, Dirty Pipe, which allowed users to overwrite sensitive files on the system. The unique characteristics of Copy Fail, including its portability and stealthiness, enhance its threat level significantly. Furthermore, it allows low-level user accounts to gain full administrative privileges, undermining the integrity of the operating system's security protocols.

Next steps are likely to involve immediate updates and patches from Linux distributors to mitigate the risks associated with this critical vulnerability.

Vocabulary List:

1. **vulnerability** //ˌvʌlnərəˈbɪləti// (noun): a weak part that can be attacked
2. **escalate** //ˈɛskəˌleɪt// (verb): to make something become more serious
3. **cryptographic** //ˌkrɪptoʊˈgræfɪk// (adjective): relating to secret codes and protecting information
4. **exploit** //ˈɛksplɔɪt// (noun): a method used to take control of something
5. **payload** //ˈpeɪˌloʊd// (noun): the data sent to cause a specific action
6. **integrity** //ɪnˈtɛgrəti// (noun): the state of being whole and unbroken

Comprehension Questions

Multiple Choice

1. What is the severity score of the vulnerability identified as CVE-2026-31431?

   Option: 5.4
   Option: 6.1
   Option: 7.8
   Option: 9.0

2. What is the codename given to the vulnerability CVE-2026-31431?

   Option: Dirty Pipe
   Option: Copy Fail
   Option: Kernel Panic
   Option: Access Denied

3. In which year was the flaw in the Linux kernel's cryptographic subsystem introduced?

   Option: 2015
   Option: 2016
   Option: 2017
   Option: 2018

4. Which module of the Linux kernel is associated with the vulnerability?

   Option: algif_aead
   Option: ext4
   Option: vfs
   Option: tcp

5. What type of script can exploit the vulnerability with a size of 732 bytes?

   Option: Bash script
   Option: Python script
   Option: Perl script
   Option: JavaScript

6. What is the first step in the exploitation process of the vulnerability?

   Option: Writing to setuid binary

Option: Opening an AF_ALG socket
Option: Executing payload
Option: Editing kernel cache

True-False

7. The vulnerability CVE-2026-31431 allows for remote exploitation.

8. Copy Fail permits unprivileged users to gain root access on Linux systems.

9. The page cache affected by Copy Fail is unique to each process.

10. Linux distributions have not issued advisories regarding the Copy Fail vulnerability.

11. A simple Python script is needed to exploit the Copy Fail vulnerability.

12. The severity score of the Copy Fail vulnerability is more than 8.

Gap-Fill

13. The logical error in the Linux kernel's cryptographic subsystem is located within the algif _____aead module, which was introduced in a code update in August _____.

14. The exploit allows a local user to manipulate the page cache of any readable file, escalating their privileges to that of a _____ user.

15. A simple _____-byte Python script can edit a setuid binary to exploit the vulnerability.

16. Exploiting the flaw requires a local user to corrupt the page cache of a setuid _____ to escalate privileges.

17. The unique characteristics of Copy Fail, including its portability and stealthiness, enhance its _____ level significantly.

18. Immediate updates and _____ from Linux distributors are likely next steps to mitigate risks associated with the vulnerability.

Answer

Multiple Choice: 1. 7.8 2. Copy Fail 3. 2017 4. algif_aead 5. Python script 6. Opening an AF_ALG socket
True-False: 7. False 8. True 9. False 10. False 11. True 12. False
Gap-Fill: 13. 2017 14. root 15. 732 16. binary 17. threat 18. patches

CATEGORY

1. Sci/Tech - LEVEL6

POST TAG

1. ESL learning
2. esl news
3. Level 6
4. Linux
5. root access
6. vulnerability

Tags

1. ESL learning
2. esl news
3. Level 6
4. Linux
5. root access
6. vulnerability

Date Created
2026/05/01
Author
aimeeyoung99