An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2605010207

NCSC Advisory

Copy Fail - Linux Kernel Local Privilege Escalation CVE-2026-31431

1 May 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-31431

Published: 2026-04-22

Vendor: All mainstream Linux distributions running kernels from 2017 to the patch date are affected, including Ubuntu, RHEL, Amazon Linux, SUSE, Debian, Fedora, and Arch.

Product: Linux

CVSS Score[1]: 7.8

Products Affected

Product	Version
Linux	72548b093ee38a6d4f2a19e6ef1948ae05c181f7 < 893d22e0135fa394db81df88697fba6032747667
Linux	72548b093ee38a6d4f2a19e6ef1948ae05c181f7 < 19d43105a97be0810edbda875f2cd03f30dc130c
Linux	72548b093ee38a6d4f2a19e6ef1948ae05c181f7 < 961cfa271a918ad4ae452420e7c303149002875b
Linux	72548b093ee38a6d4f2a19e6ef1948ae05c181f7 < 3115af9644c342b356f3f07a4dd1c8905cd9a6fc
Linux	72548b093ee38a6d4f2a19e6ef1948ae05c181f7 < 8b88d99341f139e23bdeb1027a2a3ae10d341d82
Linux	72548b093ee38a6d4f2a19e6ef1948ae05c181f7 < fafe0fa2995a0f7073c1c358d7d3145bcc9aedd8
Linux	72548b093ee38a6d4f2a19e6ef1948ae05c181f7 < ce42ee423e58dffa5ec03524054c9d8bfd4f6237
Linux	72548b093ee38a6d4f2a19e6ef1948ae05c181f7 < a664bf3d603dc3bdcf9ae47cc21e0daec706d7a5
Linux	4.14

[1] https://www.first.org/cvss/

Impact

A critical logic flaw in the Linux kernel's crypto subsystem has been publicly disclosed as CVE-2026-31431 **Copy Fail**. The vulnerability allows any unprivileged local user to escalate to root with 100% reliability. It affects virtually every mainstream Linux distribution built between 2017 and the patch date in April 2026. No race condition or system-specific offset is required — a single 732-byte Python script works unmodified across all affected systems.

Common Weakness Enumeration (CWE)[2]: CWE-669: CWE-669 Incorrect Resource Transfer Between Spheres

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review their distribution vendor's security advisories and install the relevant kernel updates.

The primary remediation is to update kernel containing commit a664bf3d603dc3bdcf9ae47cc21e0daec706d7a5 or an equivalent stable backport. The fix restores out-of-place AEAD operation, preventing page-cache pages from appearing in a writable scatterlist.

Temporary mitigation. If immediate patching is not possible, disable the algif_aead module:

```
echo "install algif_aead /bin/false" > /etc/modprobe.d/disable-algif.conf

rmmod algif_aead 2>/dev/null || true
```

- https://nvd.nist.gov/vuln/detail/CVE-2026-31431
- https://www.cve.org/CVERecord?id=CVE-2026-31431
- https://git.kernel.org/stable/c/893d22e0135fa394db81df88697fba6032747667
- https://git.kernel.org/stable/c/19d43105a97be0810edbda875f2cd03f30dc130c
- https://git.kernel.org/stable/c/961cfa271a918ad4ae452420e7c303149002875b
- https://git.kernel.org/stable/c/3115af9644c342b356f3f07a4dd1c8905cd9a6fc
- https://git.kernel.org/stable/c/8b88d99341f139e23bdeb1027a2a3ae10d341d82
- https://git.kernel.org/stable/c/fafe0fa2995a0f7073c1c358d7d3145bcc9aedd8
- https://git.kernel.org/stable/c/ce42ee423e58dffa5ec03524054c9d8bfd4f6237
- https://git.kernel.org/stable/c/a664bf3d603dc3bdcf9ae47cc21e0daec706d7a5
- https://github.com/theori-io/copy-fail-CVE-2026-31431
- http://www.openwall.com/lists/oss-security/2026/04/29/23
- https://copy.fail
- http://www.openwall.com/lists/oss-security/2026/04/29/25
- http://www.openwall.com/lists/oss-security/2026/04/29/26
- http://www.openwall.com/lists/oss-security/2026/04/30/2
- http://www.openwall.com/lists/oss-security/2026/04/30/5

- http://www.openwall.com/lists/oss-security/2026/04/30/6
- http://www.openwall.com/lists/oss-security/2026/04/30/10
- http://www.openwall.com/lists/oss-security/2026/04/30/11
- http://www.openwall.com/lists/oss-security/2026/04/30/12
- http://www.openwall.com/lists/oss-security/2026/04/30/14
- http://www.openwall.com/lists/oss-security/2026/04/30/15
- http://www.openwall.com/lists/oss-security/2026/04/30/16
- http://www.openwall.com/lists/oss-security/2026/04/30/17
- http://www.openwall.com/lists/oss-security/2026/04/30/18
- https://websec.net/blog/cve-2026-31431-linux-algifaead-page-cache-write-to-root-69f38a4ccddd2db1f520f170
- http://www.openwall.com/lists/oss-security/2026/04/30/20
- http://www.openwall.com/lists/oss-security/2026/05/01/2
- http://www.openwall.com/lists/oss-security/2026/05/01/3