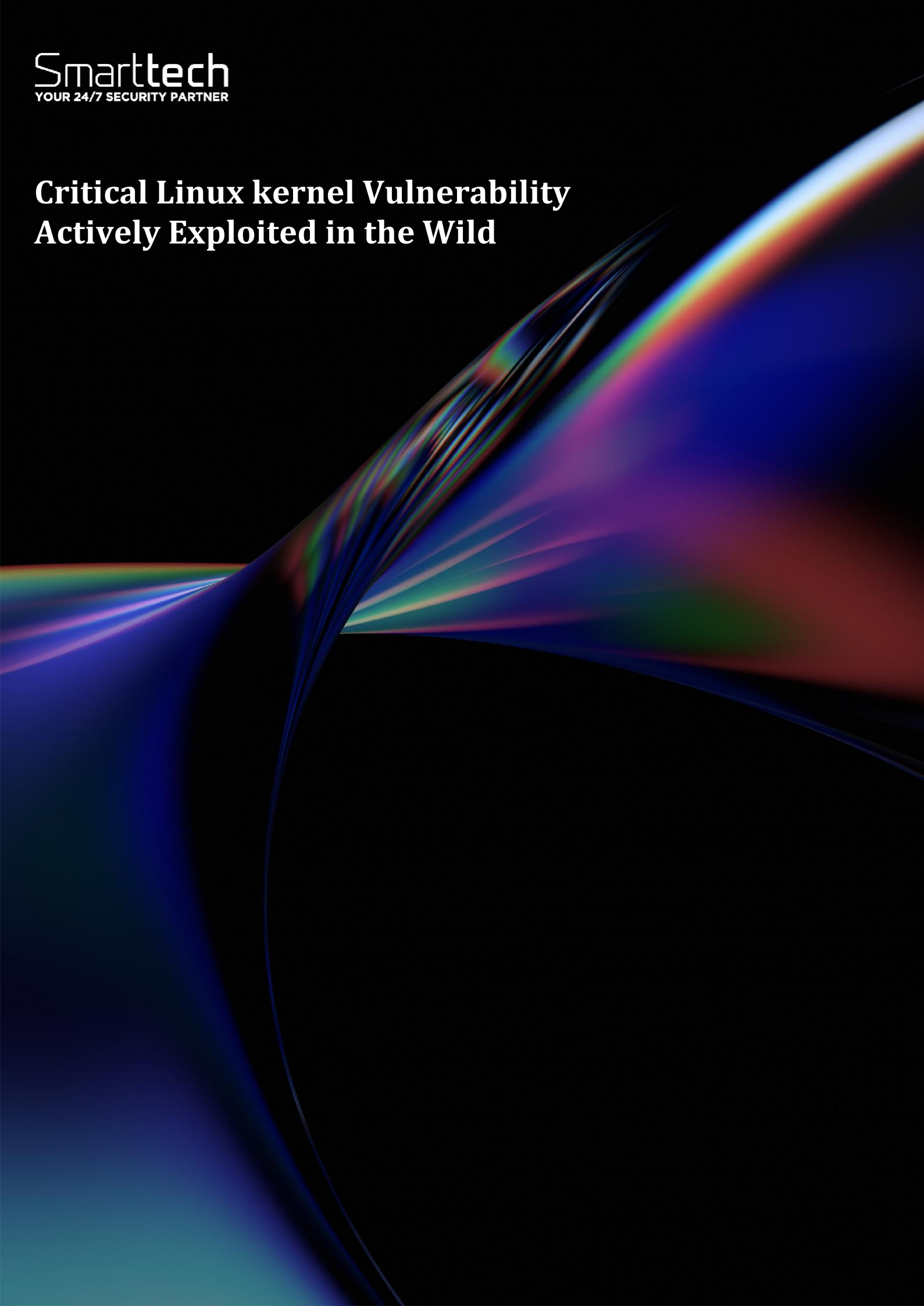
Smarttech
YOUR 24/7 SECURITY PARTNER

Critical Linux kernel Vulnerability Actively Exploited in the Wild



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	60
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-05-05
Issue Date	2026-05-01

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

A critical logic flaw has been uncovered in the Linux kernel, now confirmed to be actively exploited in real-world attacks. Tracked as CVE-2026-31431, the flaw affects all mainstream Linux distribution built between 2017 and the patch date in April 2026, including Ubuntu, RHEL, Amazon Linux, SUSE, Debian, Fedora, and Arch, and stems from an incorrect resource transfer between spheres vulnerability that could allow for privilege escalation. The issue allows an attacker to reliably trigger privilege escalation trivially by means of a 732-byte Python-based exploit, without requiring the use of complex techniques such as race conditions or memory address guessing, significantly lowering the barrier for exploitation. CISA has added the flaw to its Known Exploited Vulnerabilities (KEV) catalog after observing active exploitation attempts. The Microsoft Defender Security Research Team mentions that it's seeing preliminary testing activity that might result most likely in increased threat actor exploitation over the next few days.

Risk

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Technical summary

More details related to this vulnerability are as follows:

CVE ID	Description
CVE-2026-31431 **CVSS Base Score: 7.8**	A logic bug named "Copy Fail" in the Linux kernel permits an unprivileged local user to obtain root-level access by corrupting the kernel's in-memory page cache of any readable file, including setuid binaries. This corruption can result in arbitrary code execution with root permissions. Because the page cache represents the in-memory version of executables, modifying it

	effectively alters binaries at execution time without touching disk. The attack vector is local (AV:L), requires low privileges, and involves no user interaction, meaning any unprivileged user on a vulnerable system can attempt exploitation. As a result, it is highly impactful when chained with initial access vectors such as Secure Shell (SSH) access, malicious CI job execution, or container footholds.

Affected Products

Product	Affected 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

Recommendations

Smarttech247 team recommend the following actions be taken:

- Apply the appropriate patches or appropriate mitigations provided by the affected Linux distribution vendors to vulnerable systems immediately after appropriate testing.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Use the right Vulnerability Management Tools to assess endpoint, networks or applications for known weaknesses.
- Apply the Principle of Least Privilege to all systems and services.
- Apply advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.
- Kindly ensure that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats.

References

https://thehackernews.com/2026/05/cisa-adds-actively-exploited-linux-root.html
https://www.ncsc.gov.ie/pdfs/2605010207_CVE-2026-31431.pdf

https://github.com/theori-io/copy-fail-CVE-2026-31431/tree/main

CVE

CVE-2026-31431

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com