An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2610281063

NCSC Advisory

Linux Kernel TCP Flaw

CVE-2026-98432

30th, October 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-2026-98432

Published: 2026-10-15

Vendor: Linux

Product: Linux

CVSS Score[1]: 9.8

Products Affected

Product	Version
Linux	079096f103faca2dd87342cca6f23d4b34da8871 < b3b027ef0cd322bfa839b9aaf5b27551eea54cf6
Linux	079096f103faca2dd87342cca6f23d4b34da8871 < 95a8c8fa9f27dce64c40c41c062de7728bf34ab5
Linux	079096f103faca2dd87342cca6f23d4b34da8871 < 89b5b1eb7d633c33832b7ff2c02e19a144705036
Linux	079096f103faca2dd87342cca6f23d4b34da8871 < 742f73df544e03744f2981c467d6542fe8172a2a
Linux	079096f103faca2dd87342cca6f23d4b34da8871 < 11a03ce3c4a62d84c10ccdfe47f8075006498568
Linux	079096f103faca2dd87342cca6f23d4b34da8871 < a47406c769f72c070386985488f1c4d057df86b2
Linux	079096f103faca2dd87342cca6f23d4b34da8871 < 26d4c36d318cffbbd160884a0e4cec0da4da4936
Linux	079096f103faca2dd87342cca6f23d4b34da8871 < e3f33b0a1d89d738e2b913dab519226eaf76e15b
Linux	4.4

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

Recommendations

Impact

A critical Linux kernel IPv4 TCP race condition that can trigger use-after-free during concurrent SYN processing and request-socket migration, potentially causing information disclosure, memory corruption, or system crashes.

This affects Ubuntu, Red Hat Enterprise Linux (RHEL), and other Linux distributions. The flaw is a race condition in the code that sets up new IPv4 TCP connections. It can make the kernel read memory it has already freed, a bug type known as a use-after-free.

Common Weakness Enumeration (CWE)[2]: CWE-416: Use After Free

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

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Linux.

- https://nvd.nist.gov/vuln/detail/CVE-2026-98432
- https://www.cve.org/CVERecord?id=CVE-2026-98432
- https://git.kernel.org/stable/c/b3b027ef0cd322bfa839b9aaf5b27551eea54cf6
- https://git.kernel.org/stable/c/95a8c8fa9f27dce64c40c41c062de7728bf34ab5
- https://git.kernel.org/stable/c/89b5b1eb7d633c33832b7ff2c02e19a144705036
- https://git.kernel.org/stable/c/742f73df544e03744f2981c467d6542fe8172a2a

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

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

- https://git.kernel.org/stable/c/11a03ce3c4a62d84c10ccdfe47f8075006498568
- https://git.kernel.org/stable/c/a47406c769f72c070386985488f1c4d057df86b2
- https://git.kernel.org/stable/c/26d4c36d318cffbbd160884a0e4cec0da4da4936
- https://git.kernel.org/stable/c/e3f33b0a1d89d738e2b913dab519226eaf76e15b
- http://www.openwall.com/lists/oss-security/2026/10/30/1