An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2608250239

NCSC Advisory

Critical Linux Kernel Network Bridge Vulnerability

CVE-2026-74480

25 August 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-2026-74480

Published: 2026-08-15

Vendor: Linux

Product: Linux

CVSS Score[1]: 9.8

Products Affected

Product	Version
Linux kernel 5.10	5.10.0 < 5.10.265
Linux kernel 5.15	5.15.0 < 5.15.216
Linux kernel 6.1	6.1.0 < 6.1.183
Linux kernel 6.6	6.6.0 < 6.6.151
Linux kernel 6.12	6.12.0 < 6.12.103
Linux kernel 6.18	6.18.0 < 6.18.44
Linux kernel 7.1	7.1.0 < 7.1.8

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

Impact

A vulnerability has been resolved in the Linux kernel's network bridge multicast fast-leave functionality.

The *br_multicast_leave_group()* function iterates through a list of multicast port groups. When *br_multicast_del_pg()* deletes a matching port group, the loop can continue using a pointer associated with the deleted entry.

This condition can arise when multicast-to-unicast was previously enabled, allowing the bridge to maintain multiple port-group entries for the same port and multicast group, differentiated by their source MAC addresses.

If multicast-to-unicast is subsequently disabled, *br_port_group_equal()* matches these entries using only the port. During a fast-leave operation, one entry may then be deleted while processing continues using its stale next pointer. This can leave *mp->ports* pointing to a deleted port-group entry.

Only one matching port group needs to be removed during fast leave. The correction stops the loop immediately after *br_multicast_del_pg()* deletes the entry, preventing the kernel from dereferencing the deleted object.

Common Weakness Enumeration (CWE)[2]: N/A

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 the latest release notes and install the relevant updates from Linux.

- https://nvd.nist.gov/vuln/detail/CVE-2026-74480
- https://www.cve.org/CVERecord?id=CVE-2026-74480
- https://git.kernel.org/stable/c/d6c32e2e25a9a06ba021030e26b6d602a277eb72
- https://git.kernel.org/stable/c/482bcb85139addb4e8ac8ed10baeda3e0aad4031
- https://git.kernel.org/stable/c/1a109cc9890d017c41d77e6c82da739579c49f0b
- https://git.kernel.org/stable/c/159ad90cb929c033308bb39a2c5f8fbf393b77aa
- https://git.kernel.org/stable/c/4695430e8132420bf8de94da3eb36a6cf35fde6b
- https://git.kernel.org/stable/c/0309ebbc570000ea0df11c06b69798e5860c5f6f
- https://git.kernel.org/stable/c/4c57056ca6aace2e9f94ae9298bf49ef6b0c95e4
- https://git.kernel.org/stable/c/a39789f211b8a4125f0c70e05b30cf715f4f187d