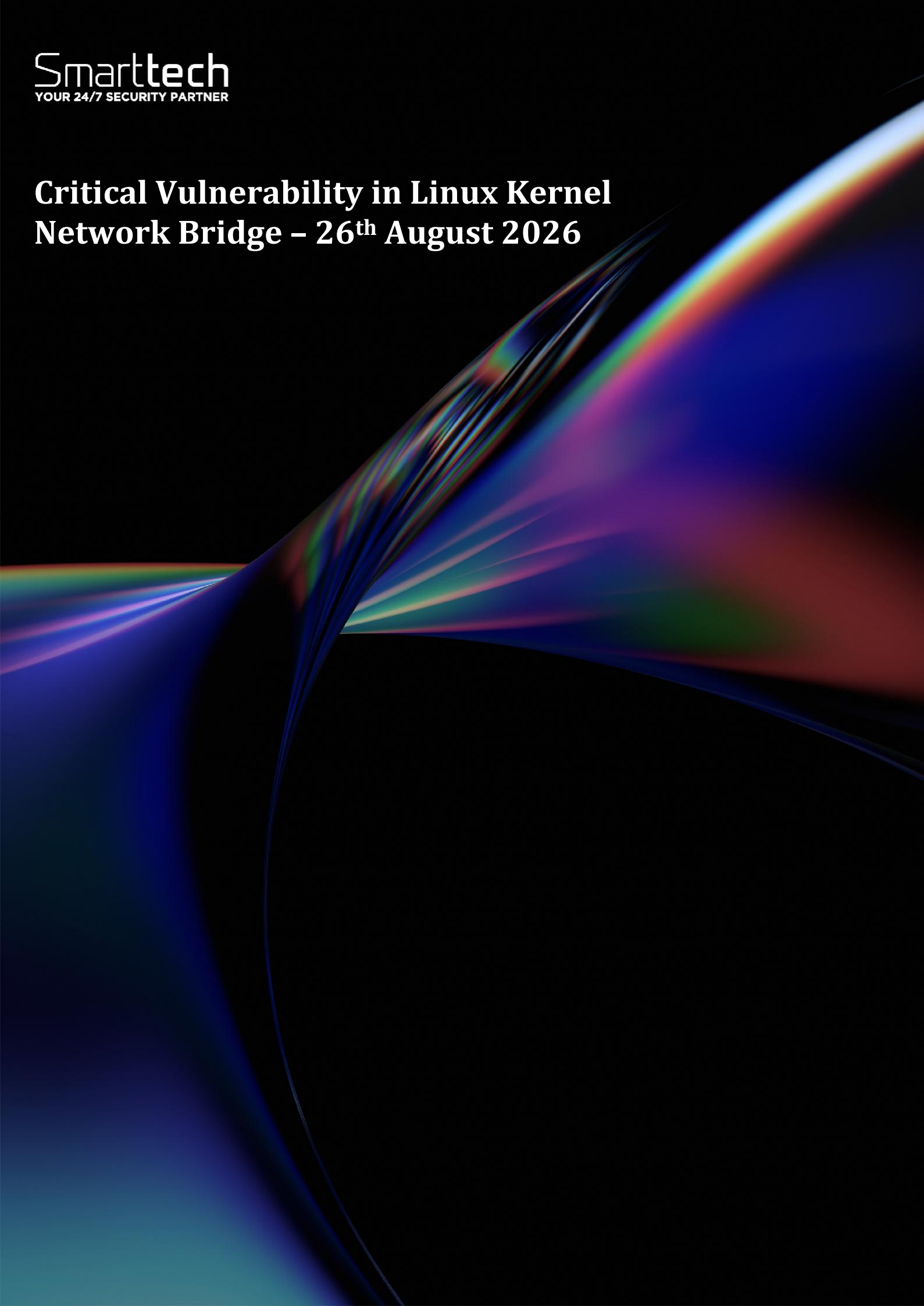
Smarttech
YOUR 24/7 SECURITY PARTNER

Critical Vulnerability in Linux Kernel Network Bridge – 26th August 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	145
Authors	Dorin Constantin Banu < constatin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-08-26
Issue Date	2026-08-25

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 privilege escalation vulnerability has been identified in the Linux kernel network bridge. Tracked as CVE-2026-74480, the flaw stems from improper handling of multicast port-group entries during bridge multicast fast-leave operations, resulting in a use-after-free condition. Under specific circumstances involving multicast-to-unicast configuration changes, the kernel may continue processing a stale pointer after a port-group entry has been deleted, leading to memory corruption. A local attacker could exploit this vulnerability to crash affected systems or escalate privileges to root.

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-2026-74480 **CVSS Base Score: 9.8**	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.

Affected Products

Product	Affected 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

Recommendations

Smarttech247 team recommend the following actions be taken:

- Apply the appropriate patches or appropriate mitigations provided by Linux 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://www.ncsc.gov.ie/pdfs/2608250239_CVE-2026-74480.pdf
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
https://securityonline.info/linux-cve-2026-74480/

CVE

CVE-2026-74480

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com