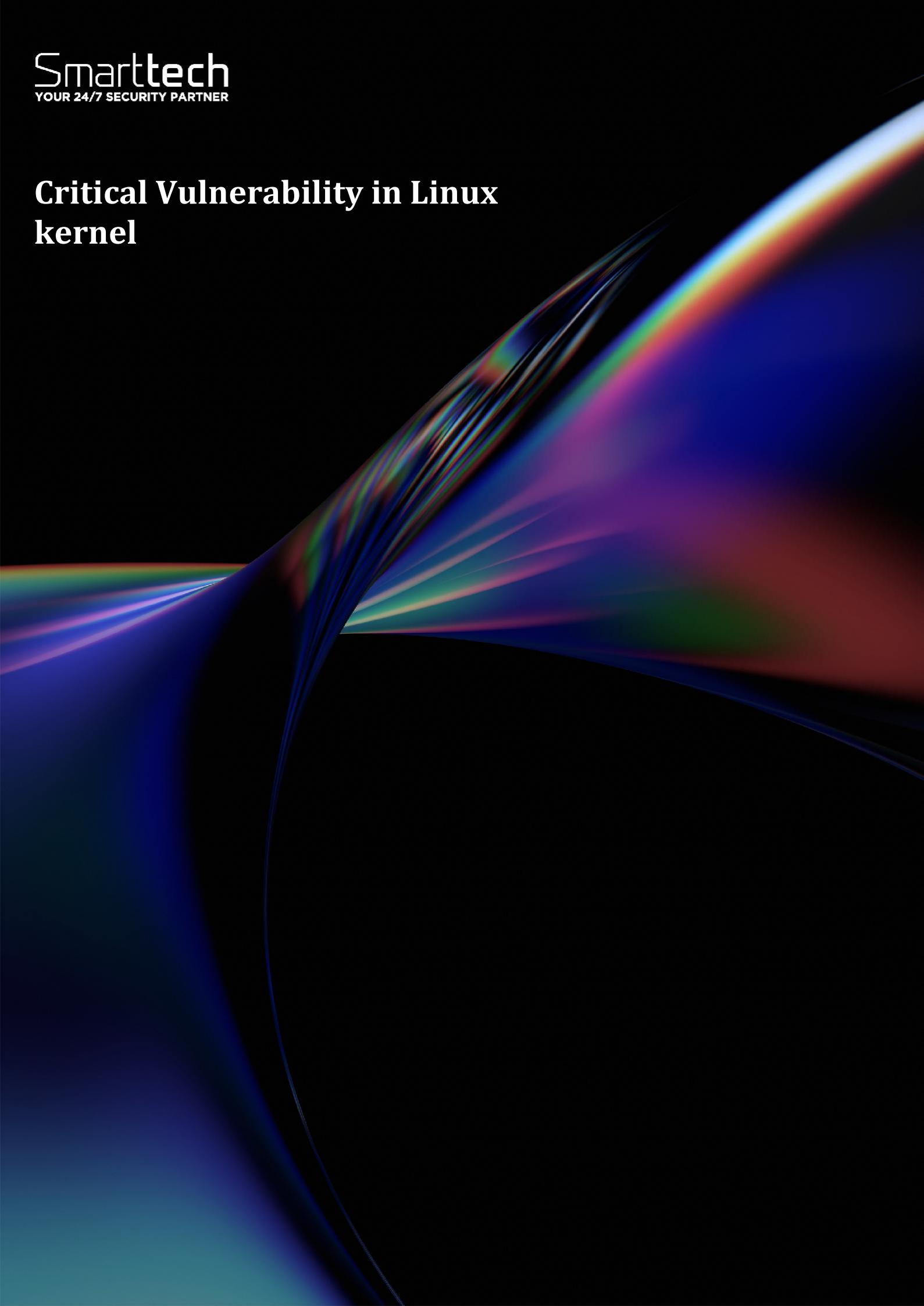
Smarttech
YOUR 24/7 SECURITY PARTNER

Critical Vulnerability in Linux kernel



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	190
Authors	Vlad Dumitrescu < vlad.dumitrescu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-11-02
Issue Date	2026-10-30

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 vulnerability, tracked as CVE-2026-98432, has been identified in the Linux kernel's IPv4 TCP networking implementation. The vulnerability is caused by a race condition that can result in a Use-After-Free memory access. This occurs when concurrent operations handling TCP connection requests access memory that has already been released.

An important consideration is that the underlying vulnerability also affects ordinary TCP connections. However, successful remote code execution has only been publicly demonstrated under specific conditions involving MPTCP listeners.

Risk

Government:

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

Businesses:

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

Affected Products

Affected Versions - Linux kernel branch	Fixed Versions
From the 4.4 branch onward, before the fixed version of each branch	5.10.272, 5.15.223, 6.1.190, 6.6.159, 6.12.113, 6.18.56, 7.2.10 and 7.3
Debian 12 (bookworm) and Debian 13 (trixie)	Fixed: 6.1.190-1 and 6.12.113-1 (bookworm also with linux-6.12 6.12.113-1~deb12u1)
SUSE Linux Micro 6.2 and openSUSE Leap 16.0	Fixed: 6.12.0-160000.40.1 or later
Oracle Linux (UEK kernels)	Fixed with errata ELSA-2026-500397 (OL7 and OL8), ELSA-2026-500398 (OL8 and OL9) and ELSA-2026-500399 (OL9 and OL10), published on 16/10/2026

Technical summary

Vulnerability ID: **CVE-2026-98432**

CVSS v3.1: 9.8 – Critical (Linux kernel CNA)
Vulnerability type: Use-After-Free (UAF) / Race Condition
Affected component: Linux kernel IPv4 TCP networking stack
Exploitation status: Proof of exploit demonstrated in a controlled environment

Security Impact

Successful exploitation could result in:

- Remote Code Execution (RCE): An unauthenticated attacker could execute arbitrary commands remotely.
- Root Privilege Escalation: The attacker could obtain the highest level of privileges on the affected Linux system.
- Full System Compromise: Attackers could modify system configurations, install malicious software, create persistent access mechanisms or compromise sensitive information.
- Lateral Movement: A compromised Linux server could potentially be used as a foothold to access other systems within the organization's network.
- Service Disruption: Exploitation of the underlying memory corruption could also result in a kernel crash or denial of service.

Recommendations

Smarttech247 team recommend the following actions be taken:

1. Perform an inventory of Linux servers, virtual machines, network appliances and cloud workloads to identify systems running potentially affected kernel versions.

2. Identify systems running MPTCP listeners, especially those exposed to the Internet or accessible from untrusted networks.

3. Install the latest security updates provided by the respective Linux distribution. Prioritize systems exposed to external networks and business-critical infrastructure.

4. Ensure that systems are restarted after kernel updates so that the patched kernel is actually loaded. Updating the kernel package without rebooting does not remove the vulnerability from the currently running kernel.

5. Where patching is not immediately possible, restrict access to affected servers to trusted IP addresses and networks. Review firewall rules and limit unnecessary inbound TCP connections.

6. If MPTCP is not required, consider temporarily disabling it to reduce the attack surface. However, disabling MPTCP alone is not sufficient to mitigate CVE-2026-98432, as the underlying vulnerability can also affect ordinary TCP connections.

References

https://www.bleepingcomputer.com/news/security/critical-linux-kernel-flaw-allows-remote-root-attacks-on-mptcp-servers/

https://thehackernews.com/2026/10/linux-kernel-tcp-flaw-with-98-cvss.html

https://beaconlab.us/en/publication/alert-2026-130-critical-vulnerability-in-the-linux-kernel-cve-2026-98432-with-a-lab-exploit-that-achieves-remote-root-access/

https://securityboulevard.com/2026/11/linux-kernel-tcp-flaw-rated-9-8-gets-a-remote-root-exploit-from-an-ai-model/

https://nvd.nist.gov/vuln/detail/cve-2026-98432

CVE

CVE-2026-98432

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com