Linux Firewall Framework Vulnerability Allows Root Privilege Escalation

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

A high-severity Linux kernel vulnerability (CVE-2026-23111) could allow a low-privileged user to gain root access on affected systems.

The flaw impacts nftables, the framework used by modern Linux firewalls to manage network traffic filtering and firewall rules. Security updates are available and organizations should patch affected Linux systems immediately.

Overview

There is a high-severity use-after-free vulnerability (CVE-2026-23111, CVSS 7.8) in the Linux kernel's nftables subsystem that could allow a low-privileged user to elevate privileges and obtain root access.

Affected Products

- Linux systems using nftables
- Linux-based firewalls using nftables
- Debian Linux
- Ubuntu Linux
- Other Linux distributions running affected kernel versions

nftables is the packet filtering framework used by modern Linux firewalls to manage firewall rules, filter network traffic, and perform network address translation (NAT). The framework replaced legacy technologies such as iptables and is commonly found on Linux servers, cloud workloads, container hosts, and network security appliances.

CVE-2026-23111 is caused by a flaw in how nftables handles certain memory operations, resulting in a use-after-free condition. A threat actor with access to a low-privileged account may be able to exploit the vulnerability to gain root access on the affected system.

The vulnerability requires local access and cannot be exploited remotely on its own. However, threat actors frequently use privilege escalation vulnerabilities after gaining an initial foothold through stolen credentials, vulnerable applications, compromised services, or container escapes. Technical details and proof-of-concept exploit code are publicly available.

Organizations operating Linux-based firewalls, servers, cloud infrastructure, container environments, and security appliances may be affected.

Aspire Protects

- **Patch** – Apply vendor-provided Linux kernel updates and verify affected systems are running patched kernel versions.
    - You may find the upstream kernel fix commit here.
- Review Linux-based firewalls, servers, cloud workloads, and container hosts for exposure.
- Restrict local access to authorized users and administrators.
- Monitor for unexpected privilege escalation activity and unauthorized root-level processes.

TTPs

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – A threat actor may exploit the vulnerability to elevate privileges and obtain root access.

Defense Evasion

- Escape to Host [T1611] – The vulnerability could be leveraged following a container escape or compromise of a containerized workload.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

The vulnerability may impact organizations that rely on Linux-based infrastructure, firewalls, cloud environments, or container platforms.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CVE-2026-23111 Common Vulnerabilities and Exposures | SUSE

NVD - CVE-2026-23111

netfilter: nf_tables: fix inverted genmask check in nft_map_catchall_activate() - kernel/git/torvalds/linux.git - Linux kernel source tree