Microsoft Publishes Advisory for Linux Kernel Privilege Escalation Flaw CVE-2026-62840



Microsoft's MSRC has published an entry for CVE-2026-62840, a Linux Kernel elevation of privilege vulnerability. The source gives no further detail, so teams should check the entry directly.

- Microsoft MSRC has published information on CVE-2026-62840.
- The flaw is classed as a Linux Kernel elevation of privilege vulnerability.
- The source gives no severity score, affected versions or patch details.
- Teams should consult the MSRC entry for updates as they appear.

What was published

Microsoft's Security Response Center has released an entry for CVE-2026-62840, described as a Linux Kernel Elevation of Privilege Vulnerability. The entry is marked as information published.

What is not yet known

The source text available to us contains only the title and the publication status. It does not state a severity rating, the affected kernel versions or distributions, whether exploitation has been observed, or whether a fix is available. We therefore do not draw conclusions on these points.

In general, an elevation of privilege flaw in an operating system kernel allows a user or process with limited rights to gain higher rights on the affected system. The practical impact depends on details that the source does not yet provide.

What to do next

Institutions that run Linux on servers, virtual machines, containers or appliances should identify where those systems are and who owns them, then follow the MSRC entry and their Linux distribution vendors for fix guidance. Decisions on priority should wait for confirmed severity and version information, and should follow your normal vulnerability and change management process.

- Confirm which Linux assets are in scope.
- Monitor the MSRC entry and vendor channels.
- Prepare to test and deploy patches once available.

What to do now

1. Inventory Linux servers, virtual machines, containers and appliances and assign owners.
2. Monitor the MSRC entry for CVE-2026-62840 and your Linux distribution vendors' advisories.
3. Add the CVE to your vulnerability register and set priority once severity and affected versions are confirmed.
4. Prepare a test and deployment window for kernel updates under change management.
5. Review privileged access and monitoring on critical Linux hosts while details are pending.