Microsoft Lists CVE-2026-113817, a Windows Human Interface Elevation of Privilege Flaw



Microsoft's update guide lists CVE-2026-113817, an elevation of privilege vulnerability in Windows Devices Human Interface. The latest revision only updates an acknowledgement; no other detail is given.

- CVE-2026-113817 is an elevation of privilege vulnerability in Windows Devices Human Interface.
- The source is Microsoft's MSRC update guide.
- The latest revision updated an acknowledgement and is described as informational only.
- The excerpt gives no severity score, affected versions or exploitation status.

What the source says

Microsoft's Security Response Center lists CVE-2026-113817 as an elevation of privilege vulnerability affecting Windows Devices Human Interface. The most recent revision of the entry updated an acknowledgement. Microsoft describes this change as informational only.

What is not stated

The available text does not include a severity rating, a CVSS score, the list of affected Windows versions, the availability of a fix, or whether the flaw is being exploited. We have therefore not assigned a risk level beyond what the source supports, and we do not infer details from the component name.

How to approach it

Elevation of privilege flaws generally matter because they can let a user or process with limited access gain higher rights on a system. Whether that applies here depends on the details in Microsoft's full entry, which security teams should read directly.

Because the latest revision is informational, it does not by itself signal a change in the required response. The practical step is to confirm how the entry applies to your Windows estate and to handle it through your normal patch and vulnerability management process once Microsoft's guidance is reviewed.

What to do now

1. Read the full CVE-2026-113817 entry in Microsoft's update guide for affected versions and fix details.
2. Check your asset inventory to identify Windows systems that may be in scope.
3. Handle the item through your standard patch and vulnerability management process once a fix is confirmed.
4. Record the review outcome for vulnerability management reporting.