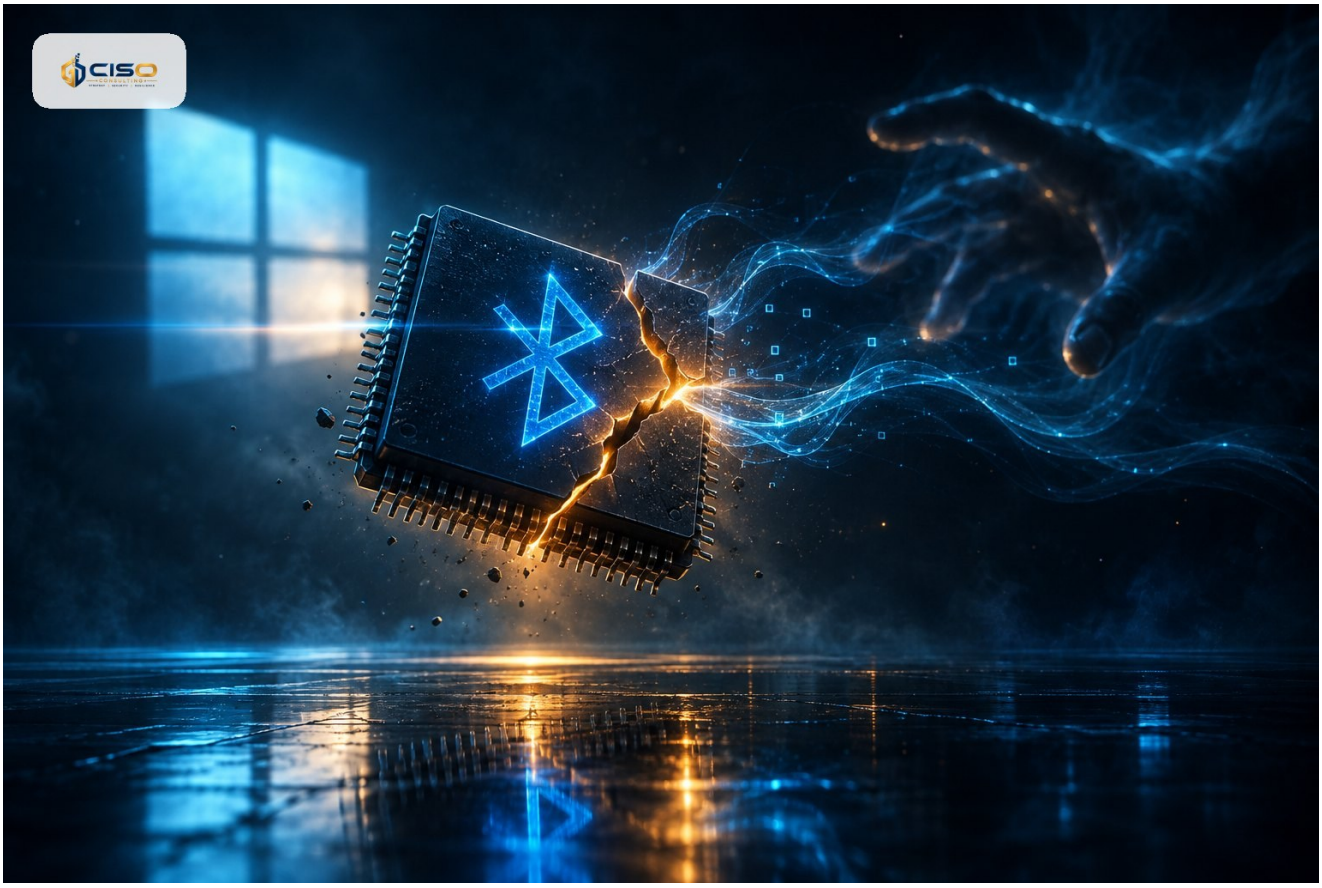
Microsoft Lists CVE-2026-83760, a Bluetooth Driver Information Disclosure Flaw



Microsoft has published CVE-2026-83760, an information disclosure vulnerability in its Bluetooth driver. The latest update only revises an acknowledgement and is informational.

- The issue is tracked as CVE-2026-83760 in the Microsoft Security Update Guide.
- It is classed as an information disclosure vulnerability in the Microsoft Bluetooth Driver.
- The latest revision updates an acknowledgement and is described as an informational change only.
- The source entry excerpt gives no severity score, affected versions or exploitation details.

What was published

Microsoft's Security Update Guide lists CVE-2026-83760, described as an information disclosure vulnerability

in the Microsoft Bluetooth Driver. The most recent change to the entry updates an acknowledgement. Microsoft states this is an informational change only.

What the source does not say

The available excerpt does not provide a severity rating, the affected Windows versions, the conditions needed to trigger the flaw, or whether it is being exploited. Those details should be read directly from the vendor entry before any risk decision is made. We have not added assumptions beyond what Microsoft has stated.

Practical implications

Because this revision does not change the technical content, it should not by itself trigger new emergency work. It is, however, a reasonable prompt to confirm that Windows endpoints are covered by your normal patch process and that the vendor entry has been reviewed for applicable fixes.

Teams that track Microsoft vulnerabilities in a register can record this CVE, note the revision as informational, and assign an owner to check the full advisory for affected products and available updates.

What to do now

1. Record CVE-2026-83760 in your vulnerability register and note that the latest revision is informational.
2. Read the full Microsoft entry to confirm affected Windows versions and available security updates.
3. Check that Windows endpoints with Bluetooth enabled are covered by your regular patching cycle.
4. Where Bluetooth is not needed on managed devices, review whether it can be disabled under your configuration baseline.