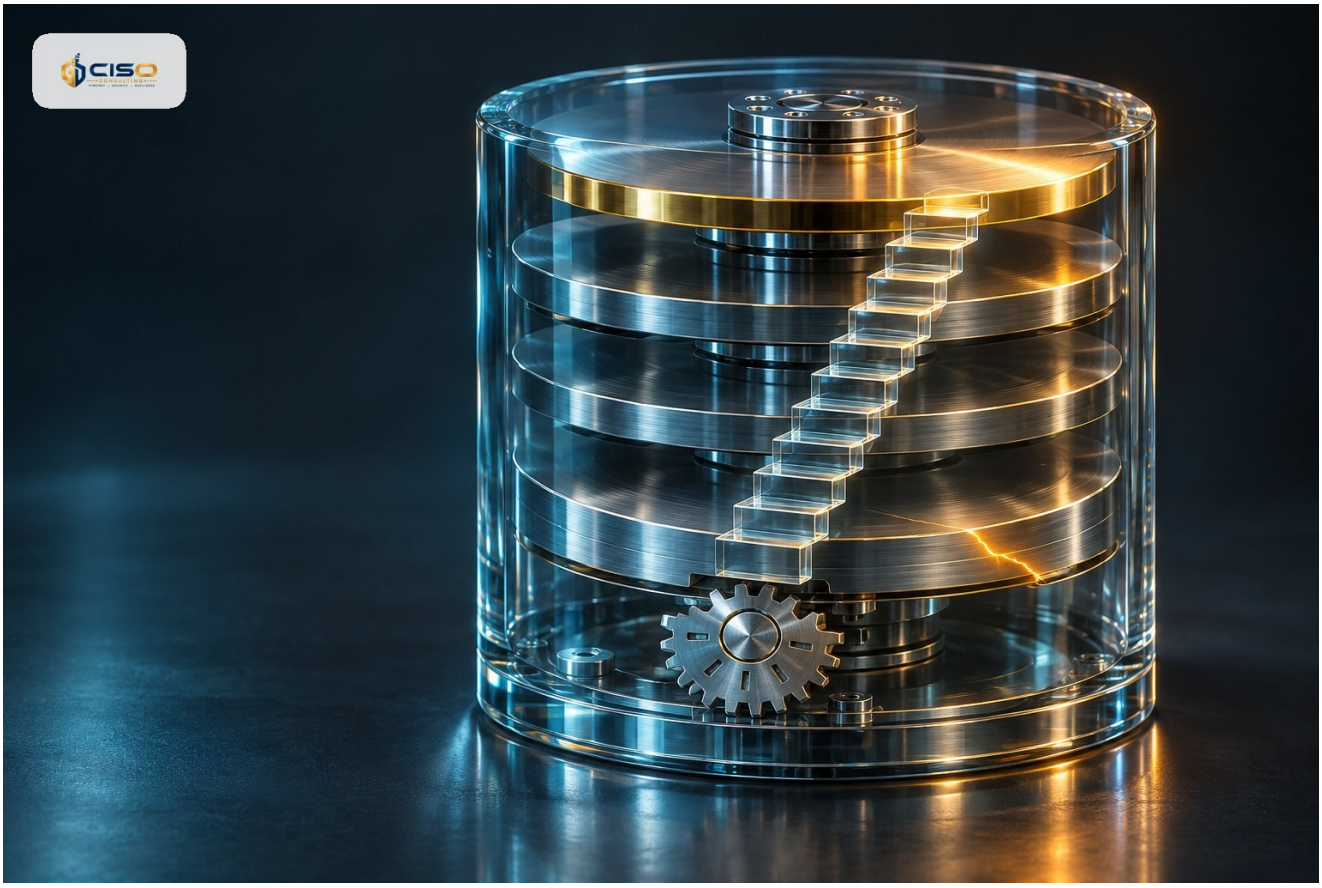
Microsoft Lists CVE-2026-95989, an Elevation of Privilege Flaw in vhdmp.sys



Microsoft's Security Update Guide lists CVE-2026-95989, an elevation of privilege vulnerability in vhdmp.sys. The latest revision only updates an acknowledgement and changes no technical content.

- The vulnerability is tracked as CVE-2026-95989 and affects vhdmp.sys.
- Its type is elevation of privilege.
- The latest revision updated an acknowledgement and is described as informational only.
- The excerpt provided does not state severity, affected versions or exploitation status.

What the source says

Microsoft's Security Update Guide carries an entry for **CVE-2026-95989**, described as an elevation of privilege vulnerability in vhdmp.sys. The most recent revision updated an acknowledgement. Microsoft labels this an informational change only, so it does not alter the technical content of the entry.

What is not stated

The excerpt we reviewed does not give a severity rating, affected product versions, patch details or any indication of exploitation. We therefore make no assessment on those points. Teams should read the full entry on the Microsoft portal for the authoritative details.

Practical reading for security teams

An elevation of privilege flaw generally matters because it can let someone who already has limited access gain broader rights on a system. Whether that applies here depends on the details in the full advisory. The revision itself requires no new urgency, but the underlying entry should be checked against your asset inventory and patch process.

- Confirm whether the entry applies to Windows builds in your estate.
- Follow your normal change and patch cycle once the vendor guidance is reviewed.
- Record the review for audit purposes.

What to do now

1. Open the full CVE-2026-95989 entry in Microsoft's Security Update Guide and note severity, affected versions and fixes.
2. Check your asset inventory for Windows systems that may be in scope.
3. Schedule any applicable update through your normal patch and change process.
4. Record the review and decision for audit evidence.