Microsoft lists CVE-2026-97761, an Excel remote code execution vulnerability



Microsoft's update guide lists CVE-2026-97761, a remote code execution vulnerability in Office Excel. The latest revision only updates an acknowledgement and changes nothing technical.

- The entry is titled Microsoft Office Excel Remote Code Execution Vulnerability and carries the identifier CVE-2026-97761.
- The latest revision updates an acknowledgement and Microsoft describes it as informational only.
- The excerpt provided gives no severity score, affected versions, exploitation status or patch details.

Microsoft has published an entry in its Security Update Guide for CVE-2026-97761, described as a remote code execution vulnerability in Microsoft Office Excel.

What the source says

The only change noted in the latest revision is an updated acknowledgement. Microsoft states that this is an informational change only, so the revision does not alter the technical content of the entry or signal new action by itself.

The excerpt available to us does not include a severity rating, the list of affected Office versions, whether the flaw is being exploited, or the fix itself. We have therefore not made any assumptions about these points.

What to do next

For teams that run Excel, the practical step is to open the full entry in Microsoft's Security Update Guide and read the affected products, severity and remediation details. Those details determine how quickly the fix must be deployed.

Organisations should check whether the update is already covered by their regular patching cycle for Office, and confirm that endpoint inventories show which versions of Excel are in use. Where the entry confirms a fix is available, schedule it according to your internal vulnerability-management policy and record the decision for audit purposes.

Until the full details are reviewed, there is no basis in the source for emergency measures. Continue to apply normal safeguards for files received from outside the organisation.

What to do now

1. Open the full CVE-2026-97761 entry in Microsoft's Security Update Guide and note affected versions, severity and fix.
2. Identify which Excel and Office versions are deployed across endpoints.
3. Confirm the fix is covered by the regular Office patching cycle and schedule it per vulnerability-management policy.
4. Document the assessment and decision for audit and regulator review.