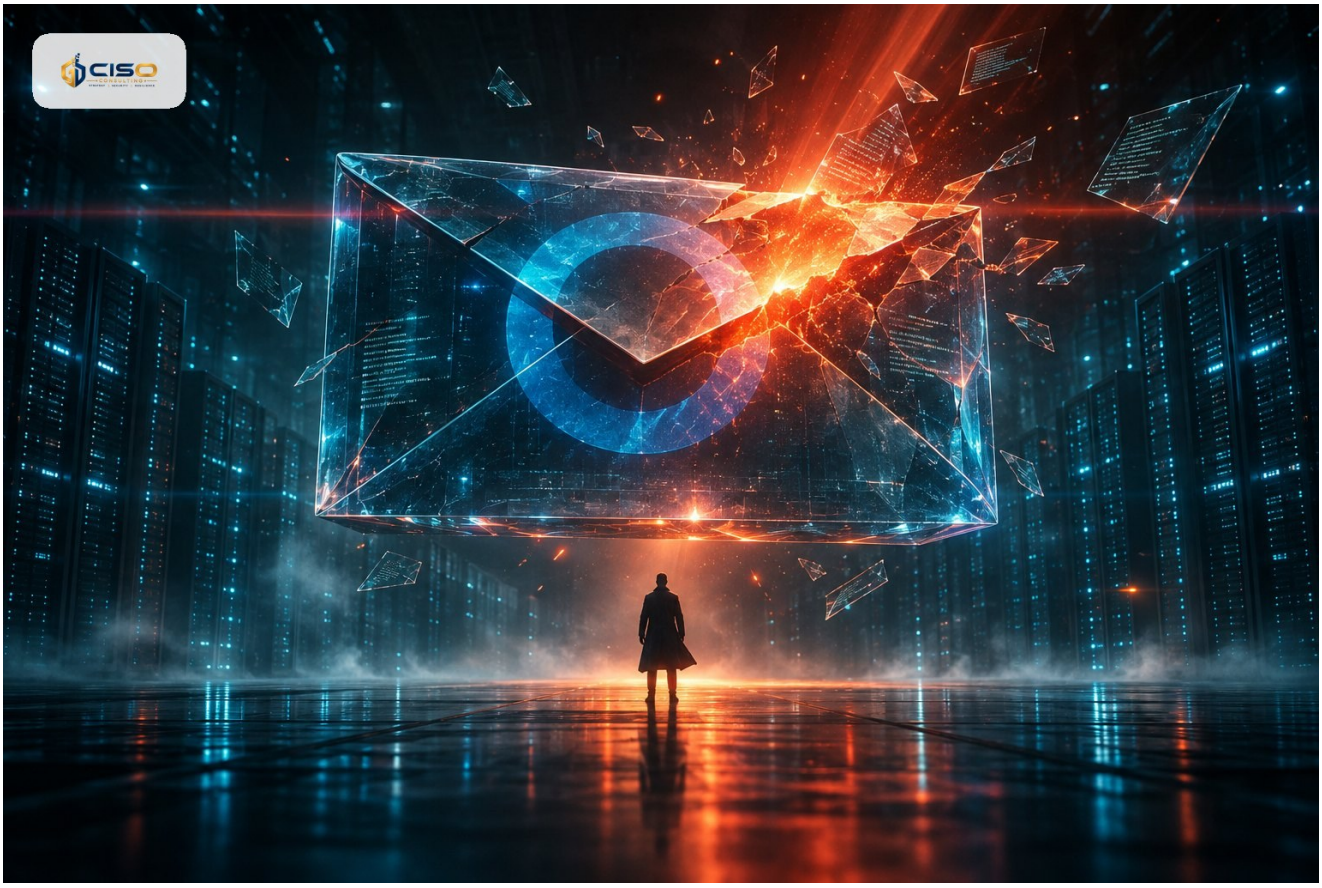
Microsoft Lists CVE-2026-97749, an Outlook Remote Code Execution Vulnerability



Microsoft has published CVE-2026-97749, a remote code execution vulnerability in Microsoft Office Outlook. The latest update to the entry only revises an acknowledgement and is informational.

- The entry is titled Microsoft Office Outlook Remote Code Execution Vulnerability and carries the identifier CVE-2026-97749.
- It is published in Microsoft's Security Update Guide (MSRC).
- The most recent revision updated an acknowledgement; Microsoft describes it as an informational change only.
- The source extract gives no severity score, affected versions or exploitation status.

Microsoft's Security Update Guide lists CVE-2026-97749, a remote code execution vulnerability affecting Microsoft Office Outlook.

What the source says

The entry identifies the issue as a remote code execution vulnerability in Outlook. The latest revision changed an acknowledgement, and Microsoft states that this is an informational change only. It does not signal a change in the technical content of the advisory.

The extract available to us does not include a severity rating, the list of affected versions, the attack conditions, the availability of a fix or any indication of exploitation. We have therefore not made assumptions about these points.

What this means for your organisation

Outlook is widely deployed across regulated institutions, so any remote code execution entry deserves a prompt check against your own estate. The practical step is to read the full entry in the Security Update Guide, confirm whether your Outlook builds are listed, and follow Microsoft's remediation guidance through your normal patch process.

Because the latest update is informational, teams that have already reviewed this CVE do not need to restart their assessment. Teams that have not yet done so should treat the review as part of routine vulnerability management and prioritise it according to the details in the official entry.

What to do now

1. Open the CVE-2026-97749 entry in Microsoft's Security Update Guide and read the affected versions and remediation guidance.
2. Check your asset inventory to confirm which Outlook versions and builds are deployed.
3. Apply the vendor's fix through your standard patch management process, prioritised by the entry's severity details.
4. Record the review and the decision taken in your vulnerability management log for audit purposes.