Microsoft Lists Excel Remote Code Execution Vulnerability CVE-2026-118302



Microsoft has published CVE-2026-118302, a remote code execution vulnerability in Microsoft Office Excel. The latest update only revises an acknowledgement; severity and fix details are not in the excerpt.

- The issue is tracked as CVE-2026-118302 and affects Microsoft Office Excel.
- It is classed as a remote code execution vulnerability.
- The most recent revision updated an acknowledgement and is informational only.
- The source excerpt gives no severity score, affected versions or patch details.

Microsoft's Security Response Center has an entry for CVE-2026-118302, described as a Microsoft Office Excel remote code execution vulnerability.

What the source says

The entry identifies the product (Microsoft Office Excel) and the vulnerability type (remote code execution). The latest revision updated an acknowledgement. Microsoft describes this as an informational change only, so it does not signal a change in the nature of the issue.

The excerpt we reviewed does not include a severity rating, affected versions, exploitation status or remediation steps. We therefore make no claims on those points.

What this means for institutions

Excel is widely used across finance, government and enterprise functions, so any remote code execution issue in it deserves a prompt check against your own estate. The practical step is to read the full advisory on the Microsoft Update Guide, confirm whether your Office builds are listed, and follow the vendor's guidance on updates.

Because the acknowledgement change carries no technical impact, teams that have already assessed this CVE need not repeat their work. Teams that have not should add it to the normal patch triage queue and prioritise it according to the severity and exploitation details published by Microsoft.

What to do now

1. Read the full CVE-2026-118302 entry in the Microsoft Update Guide.
2. Check your asset inventory for Microsoft Office Excel installations and their versions.
3. Apply Microsoft's published update or mitigation once confirmed for your builds.
4. Add the CVE to your patch management tracking with a priority based on Microsoft's severity data.
5. Remind users to be cautious with unexpected spreadsheet files until patching is complete.