

Sunday, October 4, 2026

Morning Update • Microsoft Mornings • Sun, 04 Oct 2026 12:00:00 GMT • 2:56

Maya: Good morning, and welcome to Microsoft Mornings. It is Sunday, October fourth, twenty twenty-six, and I am Maya.

Devon: And I am Devon. Coming up this morning: the clock is ticking on Windows eleven twenty-four H two, a first look at the October security update, and the biggest Patch Tuesday in Microsoft history.

Maya: Let us start with a deadline you do not want to miss. On October thirteenth, Microsoft stops issuing updates for Windows eleven, version twenty-four H two, on Home and Pro editions. After that date, no more monthly security patches, no bug fixes, no time zone updates, and no technical support.

Devon: And it is not just Windows. Office twenty twenty-one reaches its own end of support on the very same day, and unlike some products, there is no extended security update program for it. The apps will keep working, but they will never get another fix.

Maya: Microsoft's advice is simple: move to Windows eleven twenty-five H two. For most home PCs that are not managed by an I T department, the upgrade should arrive automatically through Windows Update. You still get to pick when your computer restarts, just not whether the upgrade comes.

Devon: Now to what is coming next. Microsoft has released a preview of the October security update for Windows eleven, and it is a big one. The taskbar is getting a new positioning option, the Start menu can finally be resized, and Windows Search is getting a cleaner look with clearer result categories.

Maya: There is also a new security feature called Administrator Protection, plus improvements to File Explorer, Windows Share, and Task Manager. The full rollout is expected to begin on October thirteenth, the same day twenty-four H two goes dark. Fitting, in a way.

Devon: On the security front, let us talk about last month, because it was historic. September's Patch Tuesday fixed nine hundred seventy-four security flaws, the largest Patch Tuesday on record. Two of them were zero-days already being exploited in the wild.

Maya: Both were elevation of privilege bugs in core Windows components. The first affects the Windows Advanced Local Procedure Call system, and the second targets the Windows Update stack itself. Neither had been publicly disclosed before the patches shipped, which gave defenders a head start.

Devon: Researchers also counted twenty wormable vulnerabilities in that batch, flaws that could let malware spread from machine to machine with no user interaction at all. There was also a critical remote code execution bug in Remote Desktop Services, with a severity score of nine point eight out of ten.

Maya: And the patching is not over. Just two days ago, on October second, Microsoft