

Microsoft October Windows Server updates disrupt Exchange Server operations



Microsoft confirmed that October 2026 Windows Server security updates are causing sign-in failures and mail delivery issues on some Exchange Server systems due to insufficient memory limits for Endpoint Mapper.

- October 2026 Windows Server security updates cause Outlook Web Access sign-in failures and email delivery problems on Exchange Server systems running Windows Server 2019 and later
- The issue stems from a new default memory limit of 512 simultaneous Endpoint Lookup calls introduced in the update, insufficient for Exchange Server under heavy load
- Microsoft clarified the problems are not related to October 2026 Exchange Server security updates, which should not be uninstalled
- A temporary registry-based workaround is available while Microsoft develops a permanent fix

- Impact severity varies by server load, with some Exchange servers potentially unaffected

Issue overview

Microsoft has acknowledged that security updates released in October 2026 for Windows Server are causing operational disruptions on some on-premises Exchange Server deployments. Organizations running Windows Server 2019 and later versions may experience users unable to sign in to Outlook on the web, email messages stuck in the Outbox without delivery, and mailbox access failures during replication operations.

Affected systems are reporting specific error messages including MapiExceptionMdbOffline errors with code 0x80004005 and Event ID 1006 entries in application logs. The root cause has been identified as a new default memory limit introduced in the October update that restricts Endpoint Mapper to 512 simultaneous Endpoint Lookup calls. For Exchange Server environments operating under heavy load, this limit proves insufficient.

Clarification and impact

Microsoft emphasized that these issues are unrelated to the October 2026 Exchange Server security updates themselves, urging customers not to uninstall those patches. The problem affects any Exchange version running on impacted Windows Server versions, though not all servers will experience issues equally. The severity and speed of impact depend on individual server load, with some installations potentially seeing no problems at all.

Temporary mitigation

While a permanent fix is under development, Microsoft has published a registry-based workaround. Administrators can increase the Endpoint Mapper memory limit by modifying a specific registry key through an elevated Command Prompt, followed by a system restart. After applying the workaround, organizations should monitor their Exchange environment and adjust the limit further if issues recur.

What to do now

1. Identify all on-premises Exchange Server systems running on Windows Server 2019 or later that received October 2026 security updates
2. Monitor Exchange Server application logs for Event ID 1006 and MapiExceptionMdbOffline errors indicating Endpoint Mapper memory issues
3. Test Outlook Web Access sign-in functionality and verify email delivery is functioning normally across all Exchange servers
4. Apply the registry-based workaround on affected systems by modifying the Endpoint Mapper memory limit through elevated Command Prompt and scheduling a maintenance window for system restart
5. Establish continuous monitoring of Exchange environment performance after applying the workaround to

detect any recurrence of issues

6. Document all changes made and maintain communication with Microsoft support channels for updates on the permanent fix timeline