مايكروسوفت تعالج أعطال Always On VPN الناجمة عن تحديثات Windows 11 لشهر سبتمبر



عالجت مايكروسوفت خللًا في Always On VPN سببته تحديثات Windows 11 لشهر سبتمبر 2026، عبر التحديثين التراكميين KB5127648 وKB5127646، مع حل بديل مؤقت لمن يتعذر عليه التحديث فوراً.

- أثّر الخلل في Always On VPN على Windows 11 الإصدار 24H2 وما بعده بعد تحديثات سبتمبر 2026 الأمنية.
- قد تبقى الاتصالات عالقة في حالة Connecting أو تفشل مع الخطأ «The specified port is already in use».
- يظهر الخلل عند فشل محاولة الاتصال الأولى، كما في الاختيار التلقائي للبروتوكول بين IKEv2 وSSTP.
- صدر التحديثان KB5127648 وKB5127646 يوم الثلاثاء ويعالجان المشكلة على جميع الأنظمة المتأثرة.

- الحل المؤقت: ضبط ملف VPN على بروتوكول واحد فقط، إما SSTP أو IKEv2.

عالجت مايكروسوفت مشكلة معروفة عطّلت اتصالات Always On VPN بعد تحديثات Windows 11 الأمنية لشهر سبتمبر 2026. وهذا الحل هو بديل DirectAccess للوصول عن بُعد، ويعمل في الخلفية وينشئ نفقاً آمناً إلى شبكة المؤسسة كلما اتصل الجهاز بالإنترنت.

ما الذي حدث

أقرّت مايكروسوفت بالمشكلة أول مرة في تنبيه خدمة وجّهته إلى مسؤولي تقنية المعلومات في أواخر سبتمبر. ففي أنظمة Windows 11 الإصدار 24H2 وما بعده المحدّثة بالكامل، كان فشل محاولة الاتصال الأولى يترك VPN عاجزاً عن التعافي، ويظهر ذلك عند تفعيل الاختيار التلقائي للبروتوكول أو التبديل بينه، مثل IKEv2 وSSTP. وقد تبقى الاتصالات عالقة في حالة Connecting أو تفشل، وقد تظهر في المحاولات اللاحقة رسالة «The specified port is already in use».

الإصلاح والحل المؤقت

أصدرت مايكروسوفت يوم الثلاثاء التحديثين التراكميين KB5127648 وKB5127646 لمعالجة المشكلة على جميع الأنظمة المتأثرة. وللجهات التي لا تستطيع بعد تثبيت تحديث Patch Tuesday لشهر أكتوبر 2026، تقترح مايكروسوفت تغيير ملف Always On VPN من الاختيار التلقائي للبروتوكول إلى بروتوكول واحد، إما SSTP أو IKEv2، على أن يراعي الاختيار بيئة الجهة ومتطلباتها الأمنية وطريقة النشر.

سياق أوسع

تسببت تحديثات سبتمبر أيضاً في مشكلات أخرى عالجتها مايكروسوفت بتحديثات طارئة، منها أعطال Remote Desktop Services ومشكلات Hyper-V وصوت USB. كما أكدت أن المستخدمين من غير المسؤولين قد يتعذر اتصالهم عبر Remote Desktop عند تفعيل ميزة Administrator protection.

وعملياً، ينبغي للفرق التي تعتمد على الوصول عن بُعد اختبار تحديثات أكتوبر على مجموعة تجريبية والاحتفاظ بتعديل الملف المؤقت كخيار احتياطي.

ما يجب فعله الآن

1. حدّدوا أجهزة Windows 11 الإصدار 24H2 وما بعده التي تستخدم Always On VPN مع الاختيار التلقائي للبروتوكول أو التبديل بينه.
2. اختبروا التحديث KB5127648 أو KB5127646 على مجموعة تجريبية ثم انشروه وفق إجراءات إدارة التغيير المعتمدة.
3. إن تعذّر التحديث الآن، فحوّلوا ملفات Always On VPN المتأثرة إلى SSTP فقط أو IKEv2 فقط بحسب متطلباتكم الأمنية وبيئة النشر.
4. وثّقوا أي تعديل مؤقت على الملفات كاستثناء معتمد وخططوا للتراجع عنه بعد تثبيت التحديث.
5. تحقّقوا من اتصال Remote Desktop للمستخدمين من غير المسؤولين إذا كانت ميزة Administrator protection مفعّلة.