

مايكروسوفت تعيد فتح خلل Always On VPN بعد أن صنّفته خطأً على أنه مُعالَج



أعلنت مايكروسوفت أن خلل اتصال Always On VPN في Windows 11 صنّف خطأً على أنه مُعالَج بعد تحديثات أكتوبر 2026. الإصلاح مرتقب خلال أسابيع، وثمة حل بديل مؤقت عبر تحديد بروتوكول واحد.

- أعادت مايكروسوفت حالة المشكلة من «تم الحل» إلى «مُخَفِّفة» بعد أن أغلقتها خطأً في 13 أكتوبر 2026.
- يؤثر الخلل على Windows 11 الإصدار 24H2 وما بعده عقب تحديثات سبتمبر 2026 الأمنية، عند فشل محاولة الاتصال الأولى.
- قد تبقى الاتصالات المتأثرة في حالة «Connecting» أو يظهر الخطأ «The specified port is already in use».
- الحل البديل هو تغيير ملف التعريف من الاختيار التلقائي للبروتوكول إلى SSTP فقط أو IKEv2 فقط.

أبلغت مايكروسوفت مسؤولي تقنية المعلومات بأنها صنّفت خطأً مشكلة معروفة في Always On VPN على أنها محلولة. فقد جرى تغيير الحالة إلى «Resolved» في 13 أكتوبر 2026 عقب التحديثات التراكمية لـ Windows 11 ضمن Patch Tuesday، ثم أُعيدت الآن إلى «Mitigated».

نطاق المشكلة

أقرّت مايكروسوفت بالمشكلة أول مرة في أواخر سبتمبر. وتظهر على أجهزة Windows 11 الإصدار 24H2 وما بعده بعد تثبيت تحديثات سبتمبر 2026 الأمنية، عندما تفشل محاولة الاتصال الأولى بـ Always On VPN. كما في حالة الاختيار التلقائي للبروتوكول بين IKEv2 و SSTP. وقد تبقى الاتصالات المتأثرة عالقة في حالة Connecting أو تفشل، وقد تعرض المحاولات اللاحقة رسالة تفيد بأن المنفذ المحدد قيد الاستخدام.

يعمل Always On VPN في الخلفية وينشئ أنفاقاً آمنة إلى شبكة المؤسسة كلما اتصل الجهاز بالإنترنت، ويدعم الأجهزة المنضمة إلى النطاق وغير المنضمة والمنضمة إلى Microsoft Entra ID.

الحل المؤقت والمتوقع

تقول مايكروسوفت إن الإصلاح سيُدرج في تحديث مخطط له خلال الأسابيع المقبلة. وإلى حينه، يمكن للمسؤولين تغيير ملف تعريف Always On VPN من الاختيار التلقائي للبروتوكول إلى بروتوكول واحد، إما SSTP فقط أو IKEv2 فقط، مع اختيار البروتوكول بحسب بيئة المؤسسة ومتطلبات الأمن والنشر.

وارتبطت تحديثات سبتمبر التراكمية أيضاً بمشكلات أخرى، منها أعطال Hyper-V وخدمات سطح المكتب البعيد والصوت عبر USB التي استدعت تحديثات طارئة، ومشكلة تسجيل الدخول بحسابات النطاق التي لها حل مؤقت، وخلل في النسخ الاحتياطي File History قيد المعالجة.

على المؤسسات التي تعتمد على Always On VPN للموظفين عن بُعد ألا تفترض أن تحديثات أكتوبر عالجت المشكلة، وأن تخطط وفق ذلك.

ما يجب فعله الآن

1. تحقق مما إذا كانت أجهزة Windows 11 الإصدار 24H2 وما بعده المثبت عليها تحديثات سبتمبر 2026 تستخدم الاختيار التلقائي للبروتوكول في ملفات Always On VPN.
2. عند ورود بلاغات عن اتصالات عالقة أو فاشلة، جرّب تحويل الملف إلى SSTP فقط أو IKEv2 فقط بحسب متطلبات الأمن والنشر لديكم.
3. مرّر أي تغيير في ملفات التعريف عبر إدارة التغيير ومجموعة تجريبية قبل التعميم.
4. لا تعتبروا تحديثات أكتوبر 2026 إصلاحاً للمشكلة، وتابعوا تنبيهات خدمة مايكروسوفت بشأن التحديث المرتقب.
5. زوّدوا مكتب المساندة بأعراض المشكلة ونص رسالة الخطأ لتسريع فرز بلاغات الوصول عن بُعد.
6. خططوا للعودة عن ملفات الحل المؤقت بعد صدور الإصلاح الدائم والتحقق منه.