منوعات, محطات

21 يوليو 2025 15:18 مساء

تفاصيل تحذير مايكروسوفت: هجوم سيبراني خطر يستهدف خوادم شركات وحكومات

لهجوم سيبراني واسع النطاق بعد استغلال قراصنة لثغرة أمنية كبيرة في Microsoft SharePoint تعرضت خوادم البرنامج الذي يُستخدم على نطاق واسع لتبادل وإدارة المستندات داخل المؤسسات.

وطالت الهجمات وكالات حكومية أمريكية، وولايات، وجامعات، وشركات طاقة، وشركة اتصالات آسيوية، وفقاً لما أكده مسؤولون وباحثون في الأمن السيبراني، بحسب صحيفة «واشنطن بوست».

تحقيق دولي وتعاون أمريكي وكندي وأسترالي

تجري الآن تحقيقات مشتركة بين الولايات المتحدة وكندا وأستراليا بشأن خروقات أمنية استهدفت خوادم SharePoint المستضافة محلياً داخل المؤسسات. وأشار الخبراء إلى أن عشرات الآلاف من الخوادم معرضة للخطر، كاملاً لجميع الإصدارات المتضررة حتى الآن (Patch) تحديثاً Microsoft فيما لم تصدر.

ثغرة «يوم الصفر» والتقصير المتكرر من مايكروسوفت

يعد الهجوم من نوع «يوم الصفر» لأنه استهدف ثغرة غير مكتشفة سابقاً. ويأتي ذلك بعد انتقادات سابقة لمايكروسوفت عقب اختراق صيني استهدف البريد الإلكتروني لحكومة الولايات المتحدة في عام 2023، بما في ذلك بريد وزيرة التجارة آنذاك.

Microsoft 365 خوادم محلية فقط.. وليست خوادم

المستضافة محلياً فقط، دون المساس بخدمات SharePoint أكد المسؤولون أن الهجوم اقتصر على خوادم لإصدار واحد فقط من البرنامج، بينما تظل (Patch) تصحيحاً Microsoft السحابية. وأصدرت Microsoft 365 الإصدارات الأخرى معرضة للخطر، دون توضيحات إضافية من الشركة.

آلاف الخوادم مستهدفة.. وبيانات حساسة معرضة للسرقة

المستخدم من قبل SharePoint أصدرت شركة مايكروسوفت تحذيراً بشأن «هجمات نشطة» تستهدف برنامج الوكالات الحكومية والشركات لتبادل الوثائق داخلياً، ونصحت العملاء بتثبيت التحديثات الأمنية على الفور.

محلياً تواجه خطراً SharePoint للأمن السيبراني: «أي مؤسسة تستخدم CrowdStrike قال خبراء في شركة «حقيقياً.

أن هناك محاولات لاستغلال آلاف الخوادم حول العالم قبل توفر التحديث، وتم Palo Alto Networks وأكدت شركة رصد عشرات المؤسسات المتضررة من مختلف القطاعات.

(keys) وتتيح هذه الثغرة للقراصنة سرقة بيانات حساسة، وجمع كلمات مرور، وربما الحصول على مفاتيح رقمية تمكنهم من إعادة اختراق الأنظمة حتى بعد تثبيت التحديثات.

هجمات طالت حكومات وشركات طاقة ومؤسسات تعليمية

رُصدت أكثر من 50 عملية اختراق حتى الآن، شملت شركة طاقة في ولاية أمريكية كبرى، ووكالات حكومية أوروبية، ووكالتين فيدراليتين في الولايات المتحدة، وفقا للباحثين.

وصرّح مسؤول بولاية شرقية أن المهاجمين استولوا على مستودع مستندات حكومي، مما حرم المواطنين من الوصول إليه.

ذعر أمني وانتشار مساعٍ استباقية في ولايات مثل أريزونا

في ولاية أريزونا، عقد مسؤولو الأمن السيبراني اجتماعات طارئة مع الجهات المحلية والقبلية لتقييم الوضع، في ظل حالة من الهلع حسب وصف أحد المطلعين على الوضع.

اختراقات في إسبانيا والبرازيل

من بين الضحايا: وكالة حكومية في إسبانيا، هيئة محلية في ألبوكيركي، وجامعة في البرازيل.

ورغم أن بعض الهجمات لم تتضمن حذف بيانات، إلا أن حصول القراصنة على مفاتيح التشفير يشكل خطراً دائماً بإعادة الاختراق حتى بعد التحديثات.

كيف يمكن حدوث الاختراق؟

أوضحت مايكروسوفت أن إحدى الثغرات تمكّن المهاجم المخوّل من تنفيذ عمليات انتحال عبر الشبكة.

ويعني ذلك أن المهاجم يستطيع إخفاء هويته والتظاهر بأنه جهة موثوقة (شخص، مؤسسة أو موقع إلكتروني) لاستهداف المؤسسات أو حتى التلاعب بالأسواق المالية.

توصيات الحماية العاجلة

نصحت مايكروسوفت بتثبيت التحديثات الأمنية الأخيرة فوراً.

وقالت إنه في حال تعذر تشغيل أنظمة الحماية ضد البرامج الضارة، ينبغي فصل الخوادم عن الإنترنت مؤقتاً إلى حين توفر التحديثات.

وتعمل مايكروسوفت حالياً على تطوير تحديثات خاصة بإصداري SharePoint 2016 و2019.

مايكروسوفت متهمة بالتقاعس وتكرار الأخطاء

ثغرة مشابهة في وقت سابق Microsoft أشار تقرير لوزارة الأمن الداخلي إلى أن الهجوم الحالي جاء بعد أن أصلحت من الشهر، لكن القراصنة اكتشفوا طريقة أخرى للوصول. كما انتقد الخبراء مايكروسوفت بسبب إصدارها تحديثات محدودة لا تغلق جميع المنافذ.

وتعرّضت الشركة في العامين الماضيين لاختراقات داخل شبكاتها، وسُرقت رسائل إلكترونية من كبار المسؤولين الأمريكيين بسبب ثغرات في خدماتها السحابية.