مايكروسوفت تصدر تحديثات لمعالجة 1,259 ثغرة، بينها ثغرة في Outlook مستغلة قد تكشف تجزئات NTLMv2



أصدرت مايكروسوفت تحديثات لمعالجة 1,259 ثغرة، للشهر الثاني على التوالي فوق الألف، بينها ثغرة مستغلة في Outlook قد تكشف تجزئات NTLMv2. يُنصح بإعطاء أولوية للإصلاح.

- عالجت مايكروسوفت 1,259 ثغرة، وهو الشهر الثاني على التوالي الذي يتجاوز الألف.
- تشمل الثغرات 726 في Windows و174 في Office و61 في أدوات المطورين و59 في SQL Server و27 في SharePoint Server.
- منها 165 معرّف CVE صادرة عن جهات غير مايكروسوفت.
- ثغرة في Outlook وردت على أنها مستغلة، وقد تكشف تجزئات NTLMv2.

أصدرت مايكروسوفت أحدث تحديثاتها الأمنية، وهي تعالج 1,259 ثغرة في منتجاتها. وهذا هو الشهر الثاني على التوالي الذي يتجاوز فيه عدد الثغرات 1,000.

ما الذي تشمله التحديثات

تستحوذ Windows على النصيب الأكبر بواقع 726 ثغرة، تليها Office بـ174، ثم أدوات المطورين بـ61، وSQL Server بـ59، وSharePoint Server بـ27. كما تتضمن الحزمة 165 معرّف CVE لم تصدرها مايكروسوفت نفسها.

أبرز ما يستدعي الانتباه ثغرة في Outlook وردت على أنها مستغلة فعلياً، وقد تكشف تجزئات NTLMv2، وهي بيانات اعتماد يمكن للمهاجمين إساءة استخدامها في هجمات تستهدف الهوية. ولا يذكر المقتطف المتاح رقم CVE ولا تفاصيل تقنية إضافية، لذا ينبغي الرجوع إلى نشرة مايكروسوفت الرسمية.

الأثر على فرقكم

يضع هذا الحجم الكبير ضغطاً على فرق التحديث، ما يجعل الترتيب حسب المخاطر ضرورياً. تأتي أولًا الثغرات المستغلة وتلك التي تمس برمجيات واسعة الانتشار يتعامل معها المستخدمون مثل Outlook، ثم المنتجات المكشوفة للإنترنت والخوادم مثل SharePoint Server وSQL Server.

ولأن الخطر يتعلق بتجزئات بيانات الاعتماد، فهذه فرصة مناسبة لمراجعة استخدام NTLM في بيئتكم ومدى ما قد تتيحه بيانات اعتماد مسروقة من حركة داخل الشبكة.

ما يجب فعله الآن

1. تحديد تحديث Outlook الخاص بالثغرة المستغلة من نشرة مايكروسوفت ونشره وفق جدول معجّل.
2. ترتيب بقية التحديثات حسب حالة الاستغلال ودرجة التعرّض، بدءاً بالأنظمة المكشوفة للإنترنت والخوادم.
3. مراجعة المواضع التي لا يزال يُستخدم فيها توثيق NTLM وتقييده حيثما سمحت احتياجات العمل.
4. رصد نشاط التوثيق غير المعتاد والاتصالات الصادرة التي قد تدل على التقاط التجزئات.
5. توثيق قرارات التحديث وأي تأجيل مع مبررات المخاطر لأغراض التدقيق.