تحديثات مايكروسوفت الشهرية تعالج 1,093 ثغرة، بينها ثغرة يوم صفر مستغلة في Outlook



أصدرت مايكروسوفت تحديثات نوفمبر لمعالجة 1,093 ثغرة، منها 63 حرجة. ثغرة انتحال في Outlook برقم CVE-2026-124194 مستغلة فعليًا، كما أصدرت Apple وGoogle وMozilla وAdobe تحديثات.

- عالجت مايكروسوفت 1,093 ثغرة، منها 63 حرجة، ويتيح قرابة نصف الحرجة منها تنفيذ تعليمات برمجية عن بُعد.
- الثغرة CVE-2026-124194 هي انتحال في Outlook تمس Microsoft 365 Apps for Enterprise وإصدارات Office، وهي الوحيدة التي أفادت مايكروسوفت باستغلالها فعليًا.
- يعالج Chrome 157.0.8103.50 الثغرة CVE-2026-125350، وهي ثغرة يوم الصفر السادسة في Chrome هذا العام، ويجري تحديث المتصفحات المبنية على Chromium مثل Edge.
- أصدرت Apple تحديثات خارج الدورة المعتادة لتسع ثغرات على الأقل، منها ثغرات في مجموعات iMessage، مع نقل الإصلاح إلى iOS 18.

- ينصح كريس غويتل من Ivanti بالجمع بين التحديث وإدارة التعرّض، خاصة لأجهزة الحافة وأدوات إدارة تقنية المعلومات والوصول عن بُعد.

تعالج تحديثات مايكروسوفت الشهرية لشهر نوفمبر 1,093 ثغرة في Windows والبرمجيات المدعومة. ومن بينها 63 ثغرة حرجة، يتيح نحو نصفها تنفيذ تعليمات برمجية عن بُعد، فيما تتيح 535 ثغرة رفع الصلاحيات.

ما الذي يُستغل فعليًا

أفادت مايكروسوفت بثغرة واحدة مستغلة فعليًا هي CVE-2026-124194، وهي ثغرة انتحال في Outlook. ويذكر تنبيهها أنها تؤثر في Microsoft 365 Apps for Enterprise وإصدارات من Microsoft Office.

وأصدرت جهات أخرى إصلاحات هذا الأسبوع. فقد عالج Chrome 157.0.8103.50 تسع ثغرات، منها CVE-2026-125350، وهي ثغرة يوم الصفر السادسة في Chrome هذا العام، ويجري إصلاحها كذلك في المتصفحات المبنية على Chromium مثل Edge. وأصدرت Apple تحديثات خارج الدورة المعتادة لتسع ثغرات على الأقل في iOS وiPadOS وmacOS وwatchOS وvisionOS، منها ثغرتان في مجموعات iMessage، مع نقل الإصلاح إلى iOS 18. كما عالج Firefox 160 قرابة 100 ثغرة، وأصلحت Adobe ما لا يقل عن 110 ثغرات دون دليل على استغلالها.

كيف نحدد الأولويات

أصدرت مايكروسوفت أكثر من 5,100 إصلاح أمني هذا العام، وتعزو ذلك إلى تقدم الذكاء الاصطناعي في اكتشاف الثغرات. ويشير كريس غويتل من Ivanti إلى أن 217 ثغرة فقط من نحو 95,000 ثغرة مسجلة هذا العام أُدرجت في قائمة CISA للثغرات المستغلة المعروفة. ويرى أن نحو 44% من الثغرات المستغلة توجد في أجهزة الحافة وأدوات إدارة تقنية المعلومات والوصول عن بُعد، وهي تتطلب إدارة للتعرّض إلى جانب التحديث الدوري.

ويذكّر المصدر كذلك بأخذ نسخ احتياطية للبيانات المهمة قبل تطبيق تحديثات أنظمة التشغيل.

ما يجب فعله الآن

1. إعطاء الأولوية لنشر تحديثات Microsoft 365 Apps وOffice التي تعالج CVE-2026-124194 لأنها مستغلة.
2. تحديث Chrome وEdge إلى الإصدارات التي تتضمن إصلاح CVE-2026-125350.
3. حصر أجهزة Apple والتأكد من تشغيلها أحدث إصدارات النظام، وتحديد موعد للترقية أو الاستبدال للأجهزة غير القادرة على ذلك.
4. تحديد أجهزة الحافة وأدوات الوصول عن بُعد المواجهة للإنترنت، وتأكيد تعرّضها، ومعالجة ما ثبت استغلاله أولاً.
5. أخذ نسخ احتياطية للبيانات المهمة قبل تطبيق تحديثات أنظمة التشغيل، وإبقاء بقية الإصلاحات ضمن دورة التحديث المعتادة.