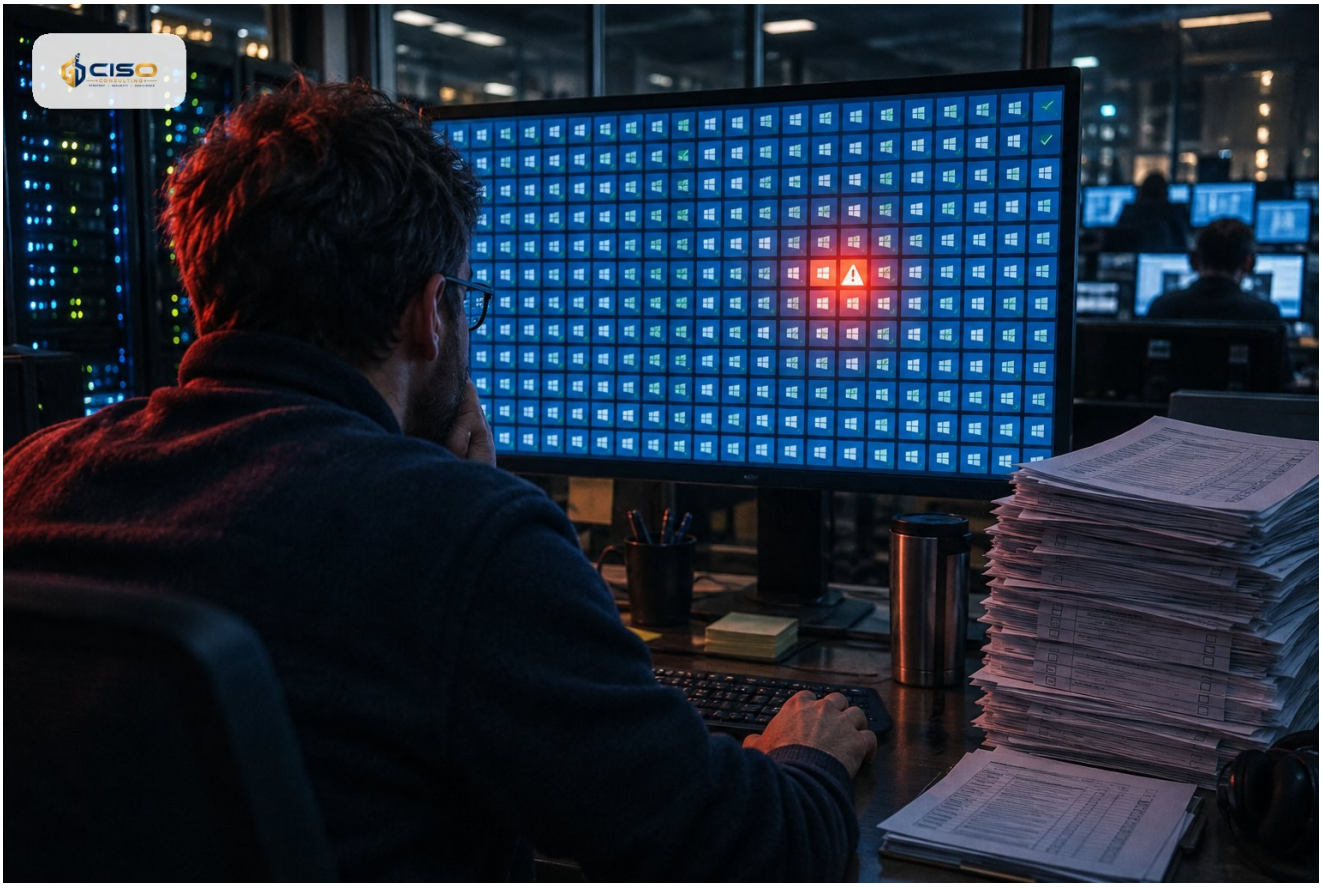
مايكروسوفت تصدر أكبر حزمة تحديثات بأكثر من 1400 إصلاح أمني، تشمل ثغرة يوم صفر مستغلة



أصلحت مايكروسوفت أكثر من 1400 ثغرة هذا الشهر، منها ثغرة Windows Shell المستغلة CVE-2026-96951. على الفرق إعطاء الأولوية للثغرات المستغلة وتخطيط طاقة الاختبار.

- أُصلح أكثر من 1400 ثغرة، متجاوزًا رقم سبتمبر القياسي البالغ نحو 1000.
- الثغرة CVE-2026-96951 في Windows Shell هي يوم الصفر الوحيد المستغل فعليًا، وتتيح تجاوز ميزة أمنية.
- ما لا يقل عن 78 ثغرة مصنفة حرجة، ومعظمها يتيح تنفيذ تعليمات برمجية.
- الثغرة CVE-2026-108398 في .NET Framework أُعلنت علنًا قبل الإصلاح ولم يُرصد استغلالها بعد.
- لا يظهر سوى 26 ثغرة لمايكروسوفت في كتالوج KEV لدى CISA هذا العام، ما يجعلها أولوية أولى معقولة.

أصدرت مايكروسوفت هذا الشهر تحديثات لأكثر من 1400 ثغرة في Windows ومنتجات أخرى. ويتجاوز هذا العدد الرقم القياسي لشهر سبتمبر البالغ نحو 1000 إصلاح، وكان بدوره يعادل قرابة عشرة أضعاف الحمل الشهري المعتاد. وأشار ساتنام نارانغ من Tenable إلى أن إجمالي العام تجاوز 4000 ثغرة، أي أكثر من 1261 ثغرة أُصلحت في عام 2020. وتعزو مايكروسوفت ارتفاع وتيرة اكتشاف الثغرات إلى نماذج اللغة الكبيرة.

الأهم أولاً

ثغرة يوم الصفر المؤكدة واحدة فقط: CVE-2026-96951، وهي تجاوز لميزة أمنية في Windows Shell يؤثر في Windows 10 وبعض إصدارات Server. وتُصنَّف 78 ثغرة على الأقل حرجة، ومعظمها يتيح للمهاجم تنفيذ تعليمات برمجية من اختياره. أما CVE-2026-108398، وهي تجاوز لميزة أمنية في .NET Framework، فقد أُعلنت علنًا قبل صدور الإصلاح. وتقول مايكروسوفت إنها غير مستغلة حتى الآن، لكن المهاجمين أتيح لهم وقت لدراستها.

الضغط التشغيلي

يحذر خبراء من أن الحزم الكبيرة ترهق الفرق التي تختبر التحديثات قبل نشرها على نطاق واسع. وذكر تايلر ريغولي من Fortra أن 26 ثغرة فقط لمايكروسوفت دخلت كتالوج الثغرات المستغلة المعروفة (KEV) لدى CISA هذا العام، واقترح البدء بمعالجتها. ودعا القادة إلى التحقق من امتلاك فرقهم الوضوح والقدرة والدعم اللازم للتحرك.

وبالنسبة إلى Windows 10، مددت مايكروسوفت التحديثات الأمنية المجانية حتى أكتوبر 2027، فتبقى هذه الأنظمة مغطاة حاليًا. وتنشر Cisco Talos ومركز SANS Internet Storm Center ملخصات تساعد في فرز الإصلاحات بحسب الخطورة والبرامج المتأثرة.

ما يجب فعله الآن

1. عالجوا CVE-2026-96951 أولاً على أنظمة Windows 10 وWindows 11 وإصدارات Server المتأثرة.
2. طابقوا ثغرات مايكروسوفت لهذا الشهر مع كتالوج KEV لدى CISA وانشروا تلك الإصلاحات أولاً.
3. جدولوا إصلاح CVE-2026-108398 في .NET Framework سريعًا لأنها معلنة علنًا.
4. خططوا لطاقة الاختبار والنشر للحجم الكبير عبر نشر تدريجي مع إمكانية التراجع.
5. تأكدوا من تسجيل أجهزة Windows 10 في برنامج التحديثات الممتدة حتى أكتوبر 2027.