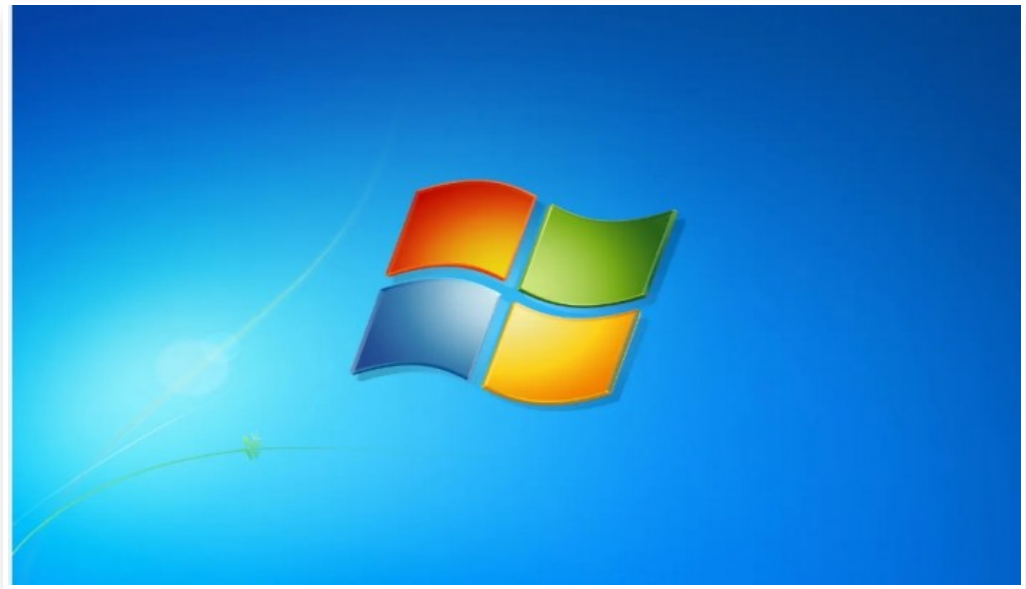
اكتشاف ثغرة أمنية في ويندوز 7 عن طريق الخطأ



الأحد 29 نوفمبر 2020 07:11 م

اكتشف باحث أمني فرنسي عن طريق الخطأ ثغرة أمنية تؤثر في نظامي التشغيل ويندوز 7 و Windows Server 2008 R2 أثناء العمل على تحديث أداة أمان ويندوز.

وتكمن الثغرة الأمنية في مفتاحي تسجيل تم تكوينهما بشكل خطأ لخدمات RPC Endpoint Mapper و DNSCache التي تعد جزءًا من كافة عمليات تثبيت ويندوز.

ويقول الباحث الأمني الفرنسي (كليمان لابرو) Clément Labro: يمكن للمهاجم المتمتع بإمكانية الوصول إلى الأنظمة الضعيفة تعديل مفاتيح التسجيل هذه لتنشيط مفتاح فرعي تستخدمه عادةً آلية مراقبة أداء ويندوز.

وعادةً ما يتم استخدام مفاتيح الأداء الفرعية لمراقبة أداء التطبيق، وبسبب دورها، فإنها تسمح أيضًا للمطورين بتحميل ملفات DLL لتتبع الأداء باستخدام أدوات خاصة.

بينما يتم عادةً في الإصدارات الحديثة من ويندوز تقييد مكتبات DLL هذه وتزويدها بامتيازات محدودة.

وقال لابرو: لا يزال من الممكن في ويندوز 7 و Windows Server 2008 تحميل مكتبات DLL خاصة تعمل بامتيازات على مستوى النظام.

ويبلغ معظم الباحثين الأمنيين مايكروسوفت عن مشكلات أمنية خطيرة مثل هذه عندما يجدونها، لكن في حالة لابرو، كان الأوان قد فات.

وقال لابرو: إنه اكتشف الثغرة بعد أن أصدر تحديثًا لأداة PrivescCheck للتحقق من التكوينات الخطأ الشائعة لأمن ويندوز، التي يمكن للبرامج الضارة إساءة استخدامها لتصعيد الامتيازات.

وأضاف تحديث أداة PrivescCheck دعمًا لمجموعة جديدة من عمليات التحقق لتقنيات تصعيد الامتيازات.

وقال لابرو: لم أعرف أن الفحوصات الجديدة تسلط الضوء على طريقة جديدة لتصعيد الامتيازات حتى بدأت التحقيق بسلسلة من التنبيهات التي تظهر عبر الأنظمة القديمة، مثل ويندوز 7، بعد أيام من إصدار تحديث الأداة.

وبحلول ذلك الوقت، كان قد فات الأوان على الباحث لإبلاغ مايكروسوفت بالمشكلة، واختار الباحث بدلاً من ذلك التدوين حول الطريقة الجديدة عبر موقعه الشخصي.

ووصل ويندوز 7 و Windows Server 2008 R2 رسميًا إلى نهاية العمر الافتراضي، وتوقفت مايكروسوفت عن توفير تحديثات الأمان المجانية.

وتتوفر بعض التحديثات الأمنية لمستخدمي ويندوز 7 من خلال برنامج الدعم المدفوع المسمى (تحديثات الدعم الموسع) ESU، لكن لم يتم إصدار تصحيح لهذه المشكلة بعد.

وليس من الواضح هل ستصلح مايكروسوفت الثغرة الأمنية الجديدة.