ثغرة يوم الصفر غير المصحّحة FastUnlock في Windows تتيح تشغيل برامج على جهاز مقفل



كُشف عن أسلوب جديد غير مصحّح باسم FastUnlock يتيح لمن يملك وصولًا مادياً إلى جهاز Windows مقفل تشغيل برامج دون تسجيل الدخول، لكن بحساب محدود الصلاحيات لا بصلاحيات المسؤول.

- FastUnlock أسلوب يوم صفر لا يتوفر له تصحيح وقت نشر الخبر.
- يتطلب وصولًا مادياً إلى جهاز Windows مقفل.
- يتيح تشغيل برامج دون تسجيل الدخول.
- يحصل المهاجم على حساب محدود فقط وليس صلاحيات المسؤول.
- نشر الأسلوب باحث يستخدم الاسمين MSNightmare وNightmare Eclipse، ويرد اسم ThreatLocker في المصدر.

ما الذي كُشف عنه

نشر باحث يستخدم الاسمين MSNightmare وNightmare Eclipse أسلوباً يحمل اسم **FastUnlock**. وبحسب الخبر، يتيح هذا الأسلوب لمن يحمل جهاز Windows مقفلًا بيده تشغيل برامج عليه دون تسجيل الدخول. والثغرة غير مصحّحة، ولذلك تُصنَّف ثغرة يوم صفر.

ما الذي يتيحه وما الذي لا يتيحه

الوصول الذي يحصل عليه المستخدم محدود؛ إذ يحصل على حساب محدود الصلاحيات وليس على صلاحيات المسؤول على الجهاز. ولا يوضح المقتطف المتاح من المصدر آلية الأسلوب التقنية ولا إصدارات Windows المتأثرة ولا أي رد من الشركة المصنّعة، ولذلك لا ينبغي افتراض شيء في هذه النقاط.

أهمية الأمر

ينصبّ الخطر أساساً على الأجهزة التي قد يصل إليها أشخاص غير مصرّح لهم: أجهزة الحاسب المحمولة أثناء السفر، والأجهزة المتروكة في أماكن مشتركة، والأجهزة المفقودة أو المسروقة. وقد يشكّل الموطئ المحدود نقطة انطلاق لخطوات لاحقة، لذا يبقى الأمن المادي وحماية الأجهزة جزءاً من الدفاع. وينبغي للفرق متابعة قنوات Microsoft بحثاً عن أي تصحيح، ومراجعة التعرض في الأثناء.

ما يجب فعله الآن

1. متابعة قنوات Microsoft الرسمية لمعرفة صدور تصحيح أو إرشادات تخفيف، والتخطيط لنشره بسرعة عند توفره.
2. تحديد أجهزة Windows المحمولة ومحطات العمل المشتركة أو الموجودة في أماكن عامة التي يُحتمل الوصول المادي إليها.
3. تعزيز الضوابط المادية: التخزين المقفل وأقفال الكابلات وقواعد واضحة بعدم ترك الأجهزة دون مراقبة.
4. التأكد من فاعلية إجراءات الإبلاغ عن الأجهزة المفقودة أو المسروقة والقفل أو المسح عن بُعد ومن معرفة الموظفين بها.
5. التحقق من تطبيق تشفير القرص الكامل وحسابات الحد الأدنى من الصلاحيات لتقليل قيمة أي موطئ قدم محدود.