استغلال SignDrop يزعم تمكين الوصول إلى صلاحيات SYSTEM عبر مشغّل CLFS في ويندوز



شيفرة استغلال علنية باسم SignDrop تزعم أن مستخدم ويندوز محلياً قادر على بلوغ صلاحيات SYSTEM عبر مشغّل CLFS. تفاصيل المصدر محدودة، ويُعامَل الأمر كخطر تصعيد صلاحيات محلي.

- صدرت هذا الأسبوع شيفرة إثبات مفهوم علنية باسم SignDrop.
- تزعم الشيفرة أن مستخدم ويندوز محلياً يستطيع الحصول على صلاحيات SYSTEM عبر مشغّل Common Log File System.
- تستهدف ميزة مصادقة السجلات التي أُضيفت إلى المشغّل العام الماضي.
- تستغل طريقة إنشاء clfs.sys لملفات مرافقة عندما تفتح عملية ذات امتيازات سجلًا معدّاً مسبقاً، مع إعادة توجيه المسار.
- لا يذكر المقتطف رقم CVE ولا حالة التصحيح.

صدرت هذا الأسبوع شيفرة استغلال علنية باسم SignDrop، وتزعم أن مستخدم ويندوز محلياً يستطيع الحصول على صلاحيات SYSTEM عبر مشغّل CLFS (Common Log File System).

ما يصفه المصدر

تستهدف شيفرة إثبات المفهوم ميزة مصادقة السجلات التي أُضيفت إلى المشغّل العام الماضي. ووفق التقرير، فهي تستغل الطريقة التي ينشئ بها clfs.sys ملفات مرافقة عندما تفتح عملية ذات امتيازات سجلًا معدّاً مسبقاً. ومن خلال إعادة توجيه المسار يُقال إن الاستغلال يتحكم في النتيجة ويصل إلى SYSTEM.

لا يتضمن المقتطف المتاح لنا رقم CVE ولا قائمة الإصدارات المتأثرة ولا حالة التصحيح ولا دليلًا على استغلال فعلي. ولم نملأ هذه الفجوات، وننصح بالتحقق منها عبر إرشادات Microsoft الرسمية.

لماذا يهم ذلك

هذه ثغرة تصعيد صلاحيات محلي، أي أن المهاجم يحتاج أولًا إلى موطئ قدم على جهاز ويندوز. والخطر العملي أن حساباً محدود الصلاحيات، حصل عليه المهاجم عبر التصيّد أو بيانات اعتماد مسروقة، قد يُرفع إلى سيطرة كاملة على الجهاز. وغالباً ما يختصر توفر شيفرة إثبات المفهوم علناً الوقت قبل أن يطوّعها آخرون.

الموقف الموصى به

لا يوجد إجراء يمنع وحده هجوماً خارجياً، لكن على المؤسسات الاستعداد: متابعة نشرات المورّد، والتأكد من أن حلول كشف النقاط الطرفية تغطي سلوك تصعيد الصلاحيات، وتقليص من يستطيع تسجيل الدخول إلى الخوادم والأجهزة الحساسة.

ما يجب فعله الآن

1. تابعوا نشرات Microsoft الأمنية بحثاً عن رقم CVE وتحديث يعالج CLFS، وجدولوا التصحيح فور توفره.
2. اسألوا مزوّد EDR عمّا إذا كانت قواعد الكشف تغطي تصعيد الصلاحيات عبر CLFS وسلوك شيفرات الإثبات العلنية.
3. قيّدوا صلاحيات تسجيل الدخول التفاعلي والبعيد على الخوادم والأجهزة الحساسة بمن يحتاجها فقط.
4. راجعوا التنبيهات الخاصة بإنشاء ملفات غير معتاد أو إعادة توجيه المسارات من عمليات ذات امتيازات على أجهزة ويندوز.
5. سجّلوا الثغرة في سجل الثغرات وحدّدوا موعداً مستهدفاً للمعالجة ضمن إجراءات إدارة التصحيحات.