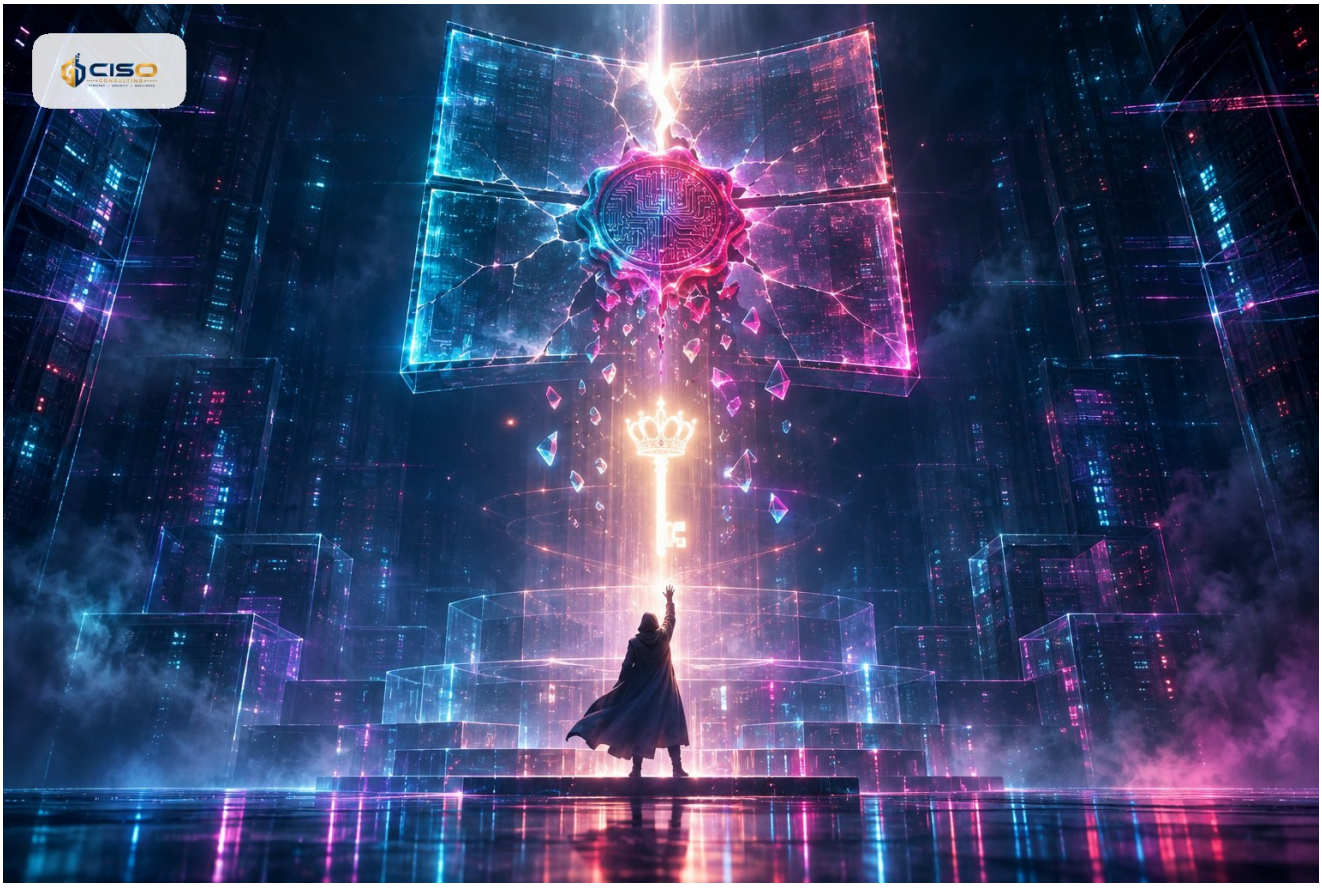
# SignDrop: ثغرة يوم صفر جديدة في Windows تتيح الحصول على صلاحيات SYSTEM



أصدر باحث يُعرف باسم Nightmare Eclipse استغلالًا لثغرة يوم صفر جديدة في Windows تُسمى SignDrop، قد تمنح المهاجمين صلاحيات SYSTEM. ولا يقدّم المصدر تفاصيل إضافية تُذكر.

- نشر الباحث Abdelhamid Naceri المعروف أيضاً باسم Nightmare Eclipse استغلالًا جديداً لثغرة يوم صفر في Windows.
- تُعرف الثغرة باسم SignDrop.
- قد يتيح الاستغلال الناجح للمهاجم الحصول على صلاحيات SYSTEM، وهي أعلى مستوى صلاحيات على جهاز Windows.
- لا يذكر النص المتاح رقم CVE أو تحديثاً أمنياً أو هجمات مؤكدة.

## ما الذي ورد في التقرير

أصدر الباحث الأمني Abdelhamid Naceri، الذي يستخدم أيضاً اسم Nightmare Eclipse، استغلالًا لثغرة غير معروفة سابقاً في Windows تحمل اسم **SignDrop**. ووفق التقرير، يمكن للاستغلال أن يمنح المهاجم صلاحيات SYSTEM.

ثغرة اليوم صفر هي ثغرة لم يتوفر لها إصلاح عند الكشف عن تفاصيلها. ولا يذكر الجزء المتاح لنا من المقال رقم CVE، ولا إصدارات Windows المتأثرة، ولا ما إذا كانت Microsoft قد استجابت، ولا ما إذا كانت الثغرة مستغلة في هجمات فعلية.

## لماذا يهم ذلك

تمثل SYSTEM أعلى مستوى من الصلاحيات على جهاز Windows. وغالباً ما يُستخدم هذا النوع من رفع الصلاحيات محلياً بعد أن يحصل المهاجم على موطئ قدم، مثلًا عبر حساب منخفض الصلاحيات مسروق أو برمجية خبيثة تعمل بصلاحيات مستخدم عادي. وبصلاحيات SYSTEM يمكن للمهاجم تعطيل أدوات الحماية أو الوصول إلى بيانات الاعتماد. كما أن نشر شيفرة الاستغلال قد يقصّر الوقت قبل أن يعيد آخرون استخدامها.

## ما العمل الآن

يُنصح بالتعامل مع الموضوع بوصفه قضية متطورة. وإلى حين صدور إرشادات من الشركة المطورة، تتمثل الأولوية العملية في تقليل فرص حصول المهاجم على موطئ قدم أولي وتحسين القدرة على اكتشاف محاولات رفع الصلاحيات. تحقق من الوضع عبر قنوات Microsoft الرسمية قبل اتخاذ إجراءات مكلفة، وتجنب تشغيل شيفرات استغلال غير موثوقة في بيئات الإنتاج.

## ما يجب فعله الآن

1. متابعة قنوات Microsoft الرسمية لمعرفة صدور نشرة أمنية ورقم CVE وتحديث لمعالجة SignDrop.
2. مراجعة صلاحيات المسؤول المحلي والحسابات منخفضة الصلاحيات على أجهزة Windows والخوادم وتقليصها.
3. التأكد من قدرة أدوات EDR والسجلات على التنبيه عند رفع الصلاحيات غير المعتاد إلى SYSTEM أو العبث بأدوات الحماية.
4. إعطاء الأولوية لضوابط منع الوصول الأولي مثل الحماية من التصيّد وقوائم السماح للتطبيقات على الأنظمة الحرجة.
5. عدم اختبار شيفرات الاستغلال المنشورة على أنظمة الإنتاج، واستخدام بيئات مختبر معزولة عند الحاجة للتحقق.