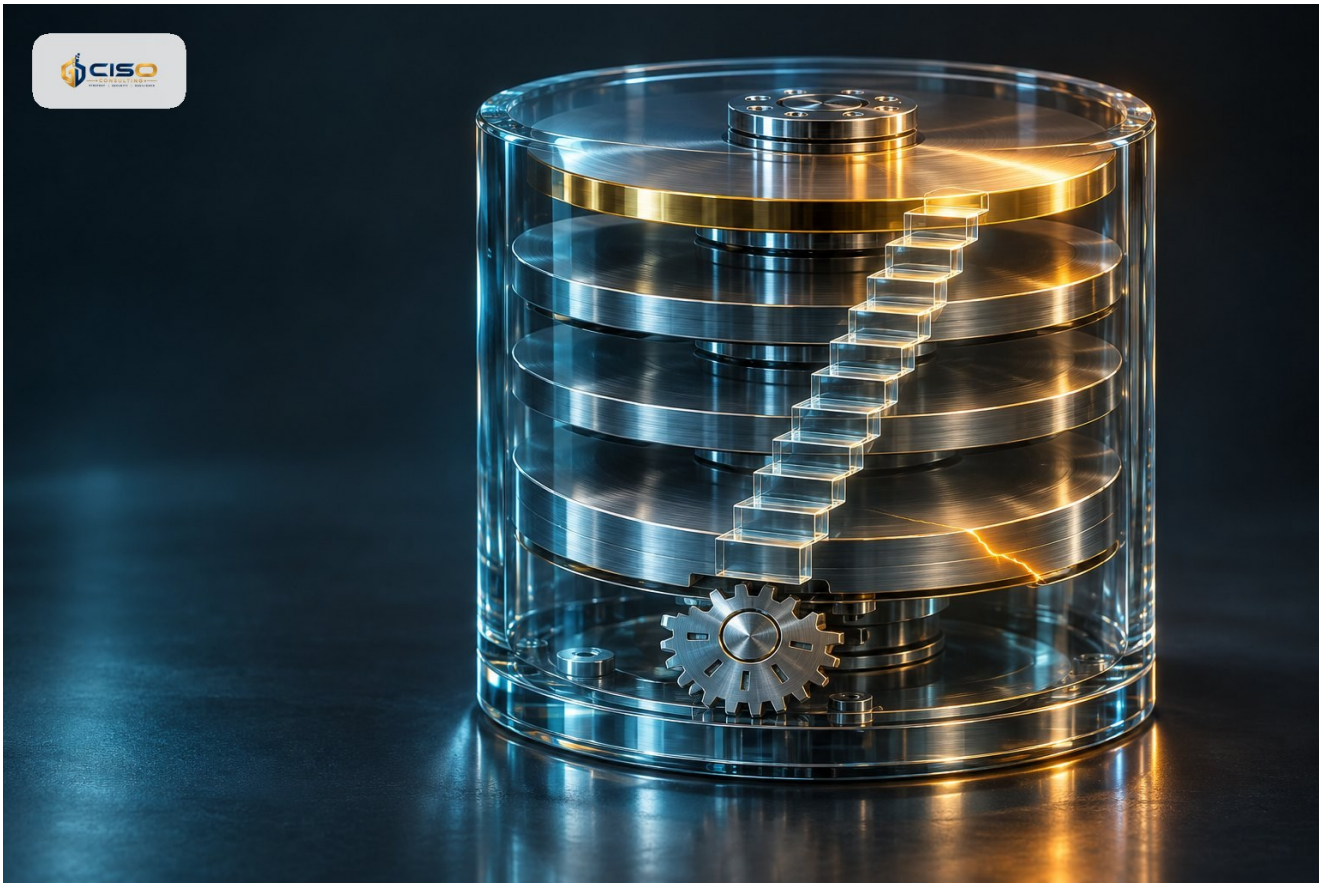
مايكروسوفت تدرج الثغرة CVE-2026-95989 لرفع الصلاحيات في مكوّن vhdmp.sys



يُدرج دليل تحديثات الأمان من مايكروسوفت الثغرة CVE-2026-95989 لرفع الصلاحيات في vhdmp.sys. والتحديث الأخير اقتصر على إقرار بالشكر دون تغيير تقني.

- تحمل الثغرة المعرّف CVE-2026-95989 وتتعلق بالمكوّن vhdmp.sys.
- نوعها رفع صلاحيات (Elevation of Privilege).
- التعديل الأخير يخص إقرارًا بالشكر ووُصف بأنه معلوماتي فقط.
- المقتطف المتاح لا يذكر درجة الخطورة ولا الإصدارات المتأثرة ولا حالة الاستغلال.

ما ورد في المصدر

يتضمن دليل تحديثات الأمان من مايكروسوفت مدخلاً للثغرة **CVE-2026-95989**، وهي ثغرة رفع صلاحيات في

المكوّن vhdmp.sys. وقد جرى في آخر مراجعة تحديث إقرار بالشكر، وتصفه مايكروسوفت بأنه تغيير معلوماتي فقط، أي أنه لا يغيّر المحتوى التقني للمدخل.

ما لم يذكره المصدر

لا يتضمن المقتطف الذي اطلعنا عليه درجة الخطورة ولا إصدارات المنتجات المتأثرة ولا تفاصيل التحديث ولا أي إشارة إلى استغلال الثغرة. لذلك لا نقدّم تقييمًا في هذه النقاط، وينبغي الرجوع إلى المدخل الكامل في بوابة مايكروسوفت للاطلاع على التفاصيل المعتمدة.

قراءة عملية لفرق الأمن

تكمن أهمية ثغرات رفع الصلاحيات عادةً في أنها قد تتيح لمن يملك وصولاً محدودًا الحصول على صلاحيات أوسع على النظام. ويتوقف انطباق ذلك هنا على تفاصيل الإشعار الكامل. ولا تستدعي المراجعة الأخيرة استعجالاً إضافيًا، لكن يُستحسن مطابقة المدخل الأصلي مع سجل الأصول وإجراءات التحديث لديكم.

- تأكدوا مما إذا كان المدخل ينطبق على إصدارات Windows في بيئتكم.
- طبّقوا التحديث وفق دورة إدارة التغيير المعتادة بعد مراجعة إرشادات الجهة المصنِّعة.
- وثّقوا المراجعة لأغراض التدقيق.

ما يجب فعله الآن

1. افتحوا مدخل CVE-2026-95989 الكامل في دليل تحديثات الأمان من مايكروسوفت ودوّنوا الخطورة والإصدارات المتأثرة والتحديثات.
2. راجعوا سجل الأصول لتحديد أنظمة Windows التي قد تكون ضمن النطاق.
3. جدولوا أي تحديث منطبق عبر إجراءات التحديث وإدارة التغيير المعتادة.
4. وثّقوا المراجعة والقرار كدليل للتدقيق.