

ثغرة حرجة لحقن الأوامر في منصة النسخ الاحتياطي Ahsay AhsayCBS



ثغرة حرجة لحقن الأوامر في نظام Ahsay AhsayCBS تتيح للمهاجمين عن بُعد تنفيذ أوامر نظام التشغيل عبر مكون النسخ المتماثل، وتتطلب تصحيحاً فورياً.

- الثغرة CVE-2026-105134 تؤثر على منصة النسخ الاحتياطي Ahsay AhsayCBS بعيب حقن أوامر في مكون النسخ المتماثل
 - يمكن للمهاجمين استغلال الثغرة عن بُعد عبر معامل عشوائي في نقطة النهاية `rps/api/json/UpdateReceivers.do/`
 - يمكن ربط الثغرة مع CVE-2026-105133 لتأثير أكبر محتمل
 - يجب على المؤسسات تطبيق تصحيحات المورد فوراً أو إيقاف استخدام المنتج إذا لم تتوفر حلول
 - حددت وكالة CISA موعداً نهائياً فيدرالياً للمعالجة في 17 أكتوبر 2026 بموجب توجيهات BOD
- 26-04

نظرة عامة على الثغرة

يحتوي نظام Ahsay AhsayCBS، وهو منصة نسخ احتياطي واستعادة من الكوارث واسعة الانتشار، على ثغرة حقن أوامر حرجية تحمل الرقم CVE-2026-105134. يكمن العيب في مكون النسخ المتماثل ويسمح للمهاجمين عن بُعد بتنفيذ أوامر نظام تشغيل عشوائية من خلال التلاعب بالمعامل العشوائي في نقطة النهاية `rps/api/json/UpdateReceivers.do/`. لا تتطلب هذه الثغرة مصادقة ويمكن استغلالها عن بُعد، مما يشكل خطراً كبيراً على المؤسسات التي تعتمد على هذه المنصة لاستمرارية الأعمال.

يمكن ربط الثغرة مع CVE-2026-105133، مما قد يوسع سطح الهجوم والتأثير المحتمل. تمكّن عيوب حقن الأوامر من هذا النوع المهاجمين من الوصول غير المصرح به إلى الأنظمة الأساسية، وسرقة البيانات الحساسة، ونشر برامج الفدية، أو إنشاء أبواب خلفية دائمة داخل شبكات المؤسسات.

السياق التنظيمي والامتثال

أصدرت وكالة CISA توجيهات بموجب BOD 26-04 لتحديد أولويات التحديثات الأمنية بناءً على المخاطر، محددةً موعداً نهائياً فيدرالياً للمعالجة في 17 أكتوبر 2026. رغم أن هذا التوجيه يطبق على الوكالات الفيدرالية الأمريكية، يجب على المؤسسات المنظمة في المملكة العربية السعودية اعتبار هذا الجدول الزمني معياراً للإجراء العاجل. يجب على المؤسسات الخاضعة لضوابط الأمن السيبراني للهيئة الوطنية للأمن السيبراني أو أطر ساما تقييم تعرضها وتنفيذ الحلول فوراً للحفاظ على الامتثال للمعايير الأمنية الإلزامية.

متطلبات الاستجابة الفورية

يجب على المؤسسات تحديد جميع نسخ Ahsay AhsayCBS في بيئتها فوراً، خاصة النشر المواجه للإنترنت. طبق التصحيحات التي يوفرها المورد فور توفرها. إذا لم تصدر الحلول بعد أو لم يمكن تطبيقها، ففكر في عزل الأنظمة المتأثرة عن الوصول للشبكة أو إيقاف الاستخدام حتى تصبح المعالجة ممكنة. وثّق جميع أنشطة المعالجة لأغراض التدقيق وأجر فحصاً جنائياً إذا اكتُشفت أي مؤشرات اختراق.

ما يجب فعله الآن

1. أجز جرداً فورياً لجميع تبيّنات Ahsay AhsayCBS في بيئتك، مع إعطاء الأولوية للنسخ المواجهة للإنترنت
2. اتصل بدعم مورد Ahsay للحصول على التصحيحات الأمنية وإرشادات التنفيذ ل CVE-2026-105134 و CVE-2026-105133
3. طبق التصحيحات التي يوفرها المورد فوراً باتباع إجراءات إدارة التغيير وبروتوكولات الاختبار
4. إذا لم تتوفر التصحيحات، عزل الأنظمة المتأثرة عن الوصول للشبكة أو أوقف الاستخدام حتى صدور الحلول
5. راجع سجلات الوصول وأجر فحصاً جنائياً على الأنظمة المتأثرة لتحديد أي مؤشرات اختراق أو تنفيذ أوامر غير مصرح به
6. وثّق جميع أنشطة المعالجة، بما في ذلك تواريخ نشر التصحيحات وتكوينات الأنظمة، لمتطلبات تدقيق الهيئة الوطنية للأمن السيبراني أو ساما