

Ahsay تُصدر تحديثات جديدة لثغرات AhsayCBS المستغلة في زرع web shells



أصدرت Ahsay Backup تحديثات لثغرتين في AhsayCBS هما CVE-2026-105133 و CVE-2026-105134، استُغلتا لزرع web shells وبرمجيات XMRIg للتعدين. وتذكر المصادر أن الإصلاحات السابقة كانت ناقصة.

- أصدرت Ahsay Backup، ومقرها سنغافورة، تحديثات أمنية لمنتج AhsayCBS.
- الثغرتان هما CVE-2026-105133 و CVE-2026-105134.
- يمكن ربطهما معاً لتجاوز المصادقة وتنفيذ أوامر عشوائية.
- استغلها المهاجمون لزرع web shells وبرمجيات XMRIg لتعدين العملات المشفرة.
- جاءت الإصلاحات الجديدة بعد إصلاحات سابقة تبين أنها غير كاملة.

أصدرت Ahsay Backup، ومقرها سنغافورة، تحديثات أمنية جديدة لمنصة AhsayCBS المخصصة لإدارة النسخ الاحتياطي. وتعالج التحديثات ثغرتين هما CVE-2026-105133 و CVE-2026-105134، وقد استغلها مهاجمون فعلاً.

ما المعروف حتى الآن

وفق التقرير، يمكن ربط الثغرتين معاً لتجاوز المصادقة ثم تنفيذ أوامر عشوائية على النظام المتأثر. وقد استخدم المهاجمون هذا المسار لزرع web shells وبرمجيات XMRIg لتعدين العملات المشفرة على خوادم مختربة. ويُفهم من العنوان أن الإصلاحات الجديدة لزمت لأن التصحيحات السابقة لم تغلق المشكلة بالكامل. لا يتضمن المقتطف المتاح تفاصيل تقنية إضافية أو أرقام الإصدارات المتأثرة أو حجم الاستغلال، لذا ينبغي الرجوع إلى نشرة الشركة المصنعة لمعرفة المزيد.

لماذا يهم ذلك

تحتفظ منصات النسخ الاحتياطي بصلاحيات مرتفعة ونسخ من بيانات حساسة، ما يجعل اختراقها أخطر من اختراق خادم عادي. ويمنح web shell المهاجم موطئ قدم دائماً، فقد لا يكفي التحديث وحده لإخراج متسلل موجود أصلاً. كما أن نقص التصحيحات السابقة يعني ألا تفترض الفرق التي طُبِّقَتْها أنها محمية.

النهج المقترح

تعاملوا مع الأمر على أنه تحديث مع تحقق: أكدوا الإصدار المستخدم، وطَبَّقُوا أحدث تحديث من المورّد، وافحصوا مؤشرات اختراق سابق قبل إعادة النظام إلى التشغيل الطبيعي.

ما يجب فعله الآن

1. حدّدوا جميع نسخ AhsayCBS في بيئكم، بما فيها التي يديرها أطراف ثالثة.
2. طَبَّقُوا أحدث تحديث من Ahsay حتى لو سبق تثبيت التصحيحات السابقة، وتأكدوا من الإصدار الناتج.
3. ابحثوا عن web shells وعمليات XMRIg على خوادم AhsayCBS قبل التحديث وبعده.
4. قيّدوا الوصول إلى واجهة الإدارة بالشبكات الداخلية الموثوقة وتجنبوا تعريضها مباشرة للإنترنت.
5. راجعوا سلامة النسخ الاحتياطية وبدّلوا بيانات اعتماد الإدارة إذا اشتّبّه بوقوع اختراق.