

ثغرة تجاوز المصادقة في Ahsay AhsayCBS تتطلب تطبيق التحديثات الأمنية فوراً



يحتوي برنامج النسخ الاحتياطي Ahsay AhsayCBS على ثغرة تجاوز مصادقة تتيح للمهاجمين عن بُعد التلاعب بمعاملات واجهة برمجة التطبيقات، مما يستوجب تطبيق تحديثات البائع فوراً أو إيقاف الخدمة.

- ثغرة مصادقة غير صحيحة في Ahsay AhsayCBS تتيح للمهاجمين عن بُعد تجاوز المصادقة عبر التلاعب بمعاملات واجهة برمجة التطبيقات
- تؤثر الثغرة على المعامل العشوائي في وظيفة checkSysPwd ضمن مكون واجهة برمجة التطبيقات
- يمكن ربط الثغرة مع CVE-2026-105134 لتأثير أكبر محتمل
- يجب على المؤسسات تطبيق تدابير البائع فوراً أو إيقاف استخدام المنتج في حال عدم توفر التحديثات

نظرة عامة على الثغرة

يحتوي Ahsay AhsayCBS، وهو حل للنسخ الاحتياطي والتعافي من الكوارث، على **ثغرة مصادقة غير صحيحة** مسجلة تحت الرقم CVE-2026-105133. تكمن الثغرة في وظيفة checkSysPwd ضمن مكون واجهة برمجة التطبيقات، حيث يمكن للمهاجمين التلاعب بالمعامل العشوائى لتجاوز آليات المصادقة عن بُعد. تشكل هذه الثغرة خطراً كبيراً على المؤسسات التي تعتمد على المنصة لعمليات النسخ الاحتياطي، خاصة عندما تكون الحالات معرضة للإنترنت.

يمكن ربط الثغرة مع CVE-2026-105134، مما قد يضخم تأثير الاستغلال الناجح. تعتبر ثغرات تجاوز المصادقة مثيرة للقلق بشكل خاص في أنظمة النسخ الاحتياطي، حيث تحمي أصول البيانات الحرجة وقدرات التعافي التي تعتمد عليها المؤسسات المنظمة لاستمرارية الأعمال.

الإجراءات المطلوبة للاستجابة

يجب على المؤسسات التي تستخدم Ahsay AhsayCBS تطبيق التدابير المقدمة من البائع فوراً وفقاً لتعليمات الشركة المصنعة. في حال عدم توفر التحديثات أو التدابير، يجب على المؤسسات إيقاف استخدام المنتج حتى يمكن تنفيذ بدائل آمنة. تتماشى هذه التوجيهات مع مبادئ تحديد أولويات التحديثات الأمنية القائمة على المخاطر. يتحمل أصحاب المصلحة مسؤولية تقييم مدى تعرض كل أصل يشغل البرنامج المتأثر للإنترنت. تتطلب الأنظمة التي يمكن الوصول إليها من الشبكات الخارجية اهتماماً فورياً وأولوية في المعالجة. يجب على المؤسسات إجراء فرز جنائي حيث يُشتبه في حدوث اختراق.

اعتبارات الامتثال

بالنسبة للمؤسسات المنظمة السعودية، تتقاطع هذه الثغرة مع التزامات امتثال متعددة. تدعم سلامة نظام النسخ الاحتياطي بشكل مباشر متطلبات استمرارية الأعمال، بينما تعد ضوابط المصادقة أساسية لأطر إدارة الوصول. يجب على المؤسسات توثيق أنشطة المعالجة وتقييم ما إذا كانت عتبات الإبلاغ عن الحوادث قد تم استيفائها بموجب الأطر التنظيمية المعمول بها.

ما يجب فعله الآن

1. إجراء جرد فوري لجميع حالات Ahsay AhsayCBS في بيئتك وتقييم مدى التعرض للإنترنت
2. تطبيق التحديثات والتدابير الأمنية المقدمة من البائع وفقاً لتعليمات الشركة المصنعة دون تأخير
3. في حال عدم توفر التحديثات، إيقاف استخدام Ahsay AhsayCBS وتنفيذ حلول نسخ احتياطي بديلة
4. إجراء فرز جنائي على الأنظمة التي يُشتبه في وصول غير مصرح به إليها، مع الحفاظ على السجلات والأدلة
5. مراجعة سجلات الوصول لوظيفة واجهة برمجة التطبيقات checkSysPwd لتحديد محاولات الاستغلال المحتملة
6. توثيق جميع أنشطة المعالجة وتقييم ما إذا كانت التزامات الإبلاغ عن الحوادث بموجب الهيئة الوطنية للأمن السيبراني أو الجهات التنظيمية القطاعية قد تم تفعيلها