

ثغرة تجاوز المصادقة في BeyondTrust Remote Support تتطلب إجراءً فورياً



يحتوي BeyondTrust Remote Support على ثغرة تجاوز مصادقة تتيح للمهاجمين عن بُعد تنفيذ عمليات ملفات على الجهاز، مما يستدعي تطبيق تدابير الحماية الفورية من المورد.

- تؤثر الثغرة CVE-2026-102764 على BeyondTrust Remote Support وتتيح تجاوز المصادقة عبر الانتحال
- يمكن للمهاجمين عن بُعد استغلال الثغرة لتنفيذ عمليات ملفات على الجهاز
- يجب تطبيق تدابير الحماية من المورد فوراً أو إيقاف استخدام المنتج في حال عدم توفر التحديثات
- على المؤسسات تقييم مدى تعرض الأصول المتأثرة للإنترنت واتباع إرشادات الترقية القائمة على المخاطر
- تشير CISA إلى إطار عمل BOD 26-04 لتحديد الأولويات مع موعد نهائي فيدرالي في 19 أكتوبر 2026

نظرة عامة على الثغرة

يحتوي BeyondTrust Remote Support، وهو حل وصول عن بُعد واسع الانتشار، على ثغرة حرجية تتمثل في تجاوز المصادقة عبر الانتحال مُتتبعة برقم CVE-2026-102764. تتيح هذه الثغرة للمهاجمين عن بُعد تجاوز ضوابط المصادقة وتنفيذ عمليات ملفات غير مصرح بها مباشرة على الجهاز. يمثل هذا خطراً كبيراً على المؤسسات التي تعتمد على المنصة للوصول عن بُعد المميز وسير عمل الدعم.

لا يتطلب استغلال الثغرة مصادقة مسبقة، مما يجعلها خطيرة بشكل خاص للأنظمة المعرضة للإنترنت. يمكن للمهاجمين الذين ينجحون في استغلال هذه الثغرة الحصول على وصول غير مصرح به إلى ملفات حساسة، مما قد يعرض سلامة وسرية الأنظمة المُدارة عبر المنصة للخطر.

الإجراءات المطلوبة

أصدرت CISA إرشادات تتطلب من المؤسسات تطبيق تدابير الحماية المقدمة من المورّد فوراً. في حال عدم توفر التحديثات أو تدابير الحماية، يجب على المؤسسات إيقاف استخدام المنتج المتأثر. تشير النشرة الاستشارية إلى التوجيه التشغيلي الملزم 04-26 من CISA، الذي يضع إطاراً قائماً على المخاطر لتحديد أولويات التحديثات الأمنية، مع موعد نهائي للامتثال الفيدرالي في 19 أكتوبر 2026.

يجب على المؤسسات إجراء فرز الأدلة الجنائية وفقاً لمتطلبات CISA المنشورة لتحديد الاختراقات المحتملة. يجب إيلاء اهتمام خاص للأصول المعرضة للإنترنت، حيث تواجه مخاطر مرتفعة.

التداعيات على المؤسسات السعودية

يجب على الجهات الخاضعة للتنظيم في المملكة التي تستخدم BeyondTrust Remote Support لإدارة الوصول المميز التعامل مع هذا الأمر كحادثة استجابة ذي أولوية. تتعارض قدرة الثغرة على تجاوز ضوابط المصادقة مباشرة مع متطلبات التحكم في الوصول ضمن أطر تنظيمية سعودية متعددة. من الضروري إجراء جرد فوري للأنظمة المتأثرة والتنسيق مع BeyondTrust للحصول على إرشادات التخفيف.

ما يجب فعله الآن

1. إجراء جرد فوري لجميع أنظمة BeyondTrust Remote Support في مؤسستك مع تدوين أرقام الإصدارات وحالة التعرض للإنترنت
2. التواصل مع دعم BeyondTrust للحصول على التحديثات أو تدابير الحماية الخاصة بـ CVE-2026-102764 وتطبيقها دون تأخير
3. في حال عدم توفر تدابير الحماية، عزل الأنظمة المتأثرة عن الإنترنت أو إيقاف الاستخدام حتى صدور التحديثات
4. إجراء فرز الأدلة الجنائية على جميع أجهزة BeyondTrust لتحديد مؤشرات الاختراق أو الوصول غير المصرح به للملفات
5. مراجعة سجلات الوصول للكشف عن أنماط مصادقة شاذة أو عمليات ملفات قد تشير إلى محاولات استغلال
6. تحديث إجراءات الاستجابة للحوادث وإخطار الجهات المعنية بما في ذلك المركز الوطني الإرشادي للأمن

السيبراني في حال اكتشاف أو الاشتباه في اختراق