

CISA تنصح باتخاذ إجراءات فورية بشأن ثغرة دعم BeyondTrust عن بُعد



حددت CISA ثغرة حرجية في تجاوز المصادقة في دعم BeyondTrust عن بُعد، داعيةً المؤسسات لتطبيق التصحيحات وترقية أنظمتها للتخفيف من المخاطر.

- ثغرة حرجية تؤثر على إصدارات دعم BeyondTrust عن بُعد 26.2.3 وما قبلها.
- التصحيحات متاحة للإصدارات المدعومة؛ يجب ترقية الإصدارات القديمة.
- المهاجمون الإلكترونيون يستغلون هذه الثغرة بنشاط.
- يجب على المؤسسات تقييد الوصول الخارجي إلى أجهزة دعمها عن بُعد.
- إجراء تحقيقات جنائية إذا تم الاشتباه في حدوث اختراق.

نظرة عامة

أبلغت CISA عن ثغرة حرجية في تجاوز المصادقة في دعم BeyondTrust عن بُعد، تؤثر على الإصدارات 26.2.3 وما قبلها. المؤسسات التي تستخدم هذه الإصدارات معرضة لخطر الاستغلال من قبل المهاجمين الإلكترونيين الذين يمكنهم الوصول غير المصرح به وزيادة الامتيازات.

الإجراءات الموصى بها

يجب على المؤسسات التي لديها أجهزة دعم عن بُعد مستضافة ذاتيًا اتخاذ إجراءات فورية لتصحيح أنظمتها. التصحيح BT26-05-RS متاح، ولكن يجب على أولئك الذين يستخدمون إصدارات أقدم أولاً ترقية إلى إصدار مدعوم (24.3.1 أو أحدث) لتطبيق التصحيح. من الضروري أيضًا تقييد الوصول الخارجي إلى الخدمات الضرورية فقط وتقييد الوصول الإداري إلى الشبكات الموثوقة.

في حالة الاشتباه في حدوث اختراق، يجب على المؤسسات إجراء تحقيقات شاملة في الشبكة والذاكرة لجمع الأدلة. يشمل ذلك عزل أي أجهزة مخترقة وجمع السجلات ذات الصلة للتحليل. بعد التحقيق الجنائي، يجب على المؤسسات إعادة بناء أنظمتها من حالة معروفة جيدة، وتطبيق التصحيحات اللازمة، وتدوير جميع بيانات الاعتماد المخزنة لتعزيز الأمان.

ما يجب فعله الآن

1. تطبيق التصحيح BT26-05-RS على الفور إذا كنت تستخدم إصدارًا مدعومًا.
2. ترقية إلى الإصدار 24.3.1 أو أحدث إذا كنت تستخدم إصدارًا قديمًا.
3. تقييد الوصول الخارجي إلى الخدمات الضرورية فقط.
4. تقييد الوصول الإداري إلى الشبكات الموثوقة.
5. إجراء تحقيقات جنائية إذا تم الاشتباه في حدوث اختراق.