Arista تصدر تحديثًا لثغرة يوم الصفر المستغلة في VeloCloud Orchestrator (CVE-2026-114625)



أصدرت Arista تحديثًا للثغرة الحرجة CVE-2026-114625 في VeloCloud Orchestrator المحلي، وهي ثغرة حقن SQL مستغلة فعليًا تتيح لأي مستخدم موثق رفع صلاحياته. يُنصح بالتحديث وتطبيق إجراءات الحماية المؤقتة.

- الثغرة CVE-2026-114625 حرجة، من نوع حقن SQL، تؤثر في VCO (VeloCloud Orchestrator) المحلي وتُستغل في هجمات فعلية.
- يستطيع مستخدم موثق بصلاحيات أساسية رفع صلاحياته إلى مشغّل والظهور كمستخدم «superuser operator» محلي.
- رقّعت Arista بالفعل نسخ VCO المستضافة التي تعمل بالإصدارات 5.2.3.18 أو أحدث، و6.1.3.10 أو أحدث، و6.4.2.12 أو أحدث.
- حددت Arista عنواني IP رُصدا في الهجمات: 82.197.86[.]74 و54.50.151[.]38.

- عالجت Arista هذا العام ثلاث ثغرات يوم صفر مستغلة أخرى في EOS وVCO المحلي.

أصدرت Arista Networks تحديثات أمنية لمعالجة ثغرة يوم صفر مستغلة فعليًا في VeloCloud Orchestrator (VCO) المحلي، وهو بوابة ويب تُستخدم لإعداد شبكات VeloCloud SD-WAN وأجهزة الحافة المرتبطة بها ومراقبتها وإدارتها.

ما الذي تتيحه الثغرة

الثغرة المعرّفة بالرمز CVE-2026-114625 مصنّفة حرجة. يستطيع المهاجم الذي يملك صلاحيات أساسية ويصل إلى واجهة الويب ولديه جلسة موثقة صالحة استغلال حقن SQL منخفض التعقيد، دون تفاعل من المستخدم، لرفع صلاحياته. وبحسب Arista يمكن لأي مستخدم موثق الحصول على صلاحيات المشغّل والظهور كمستخدم «superuser operator» محلي، والوصول إلى وظائف مخصصة للاستخدام الداخلي فقط. وقد يمس الاستغلال سرية المنسّق وسلامته وتوافره، وكذلك البيانات التي يديرها.

رقّعت Arista بالفعل النسخ المستضافة من VCO التي تعمل بالإصدارات 5.2.3.18 أو أحدث، و6.1.3.10 أو أحدث، و6.4.2.12 أو أحدث. وهذه رابع ثغرة يوم صفر مستغلة تعالجها الشركة هذا العام في EOS وVCO المحلي، بعد CVE-2026-7473 وCVE-2026-16812 وCVE-2026-93952.

إجراءات مؤقتة توصي بها Arista

إلى حين تطبيق التحديثات، توصي Arista بحصر الوصول إلى واجهة VCO في شبكات الإدارة، ومراقبة الاتصالات الصادرة من عناوين خبيثة معروفة، ومراجعة نشاط المسؤولين الأخير بحثًا عن تغييرات غير معتادة. كما تقترح فحص سجلات وصول الويب بحثًا عن مسارات تشبه عناوين URL على نحو غير معتاد، أو أحرف مرمّزة، أو إشارات إلى خدمات محلية أو داخلية، أو معدلات طلبات مرتفعة. ويجب حجب العنوانين 74[.]82.197.86 و38[.]54.50.151.

وعند الاشتباه باختراق، توصي Arista بحفظ سجلات وصول الويب وسجلات التطبيق الخلفي والنظام وقاعدة البيانات والأختام الزمنية لنظام الملفات قبل المعالجة متى أمكن تشغيليًا، والتواصل مع مركز المساعدة الفنية TAC التابع لـ Arista.

ما يجب فعله الآن

1. حصر جميع نسخ VCO المحلية والتحقق من إصداراتها مقارنة بالإصدارات المصححة التي حددتها Arista، وتطبيق التحديث فور سماح إدارة التغيير.
2. حصر الوصول إلى واجهة VCO في شبكات الإدارة المخصصة إلى حين اكتمال التحديث.
3. حجب العنوانين 74[.]82.197.86 و38[.]54.50.151 والبحث في السجلات السابقة عن أي اتصال منهما.
4. مراجعة سجلات وصول الويب ونشاط المسؤولين الأخير بحثًا عن أحرف مرمّزة وإشارات لخدمات داخلية ومعدلات طلبات مرتفعة وتغييرات غير متوقعة.
5. عند الاشتباه باختراق، حفظ سجلات الويب والتطبيق والنظام وقاعدة البيانات والأختام الزمنية قبل المعالجة، والتواصل مع TAC لدى Arista، واتباع إجراءات الاستجابة للحوادث والإبلاغ للجهات التنظيمية.