Arista تحذّر من ثغرة يوم الصفر حقن SQL في VeloCloud Orchestrator يجري استغلالها فعليًا



أفادت Arista بأن مهاجمين يستغلون ثغرة يوم الصفر من نوع حقن SQL في VeloCloud Orchestrator، منصة إدارة VeloCloud SD-WAN. ويمكن لأي مستخدم يملك حساب دخول، ولو للقراءة فقط، رفع صلاحياته إلى مشغّل.

- نشرت Arista تنبيهًا في 22 أكتوبر يؤكد وجود استغلال فعلي للثغرة.
- الثغرة من نوع حقن SQL وهي يوم صفر في VCO (VeloCloud Orchestrator)، نظام الإدارة المركزي لشبكات VeloCloud SD-WAN.
- يكفي لاستغلالها حساب دخول صالح، بما في ذلك حساب عميل بصلاحية قراءة فقط.
- يمنح الاستغلال الناجح صلاحيات المشغّل، وهي أعلى مستوى تحكم في المنسّق.

ما الذي أُعلن

ذكرت Arista في تنبيه بتاريخ 22 أكتوبر أن مهاجمين يستغلون بالفعل ثغرة يوم الصفر من نوع حقن SQL في VeloCloud Orchestrator (VCO). ويمثّل VCO نظام الإدارة المركزي لشبكات VeloCloud SD-WAN، أي أنه يتحكم في إعداد الشبكة وتشغيلها على نطاق واسع.

أهمية الأمر

تخفّض هذه الثغرة مستوى الصعوبة أمام المهاجم بشكل كبير. فأي شخص يستطيع تسجيل الدخول إلى المنسّق يمكنه رفع صلاحياته إلى **مشغّل** (operator)، وهو أعلى مستوى تحكم، ويشمل ذلك حسابات العملاء ذات صلاحية القراءة فقط. لذلك لا يحتاج المهاجم إلى موطئ قدم إداري، بل إلى بيانات دخول صالحة من أي نوع.

وبالنسبة للجهات التي تعتمد SD-WAN لربط الفروع ومراكز البيانات والخدمات السحابية، فإن اختراق المنسّق حدث عالي الأثر. ولا يتضمن المقتطف المتاح تفاصيل تقنية إضافية أو الإصدارات المتأثرة أو معلومات التصحيح، ولذلك ينبغي التحقق منها مباشرة من تنبيه Arista.

النهج المقترح

يُنصح بالتعامل مع الأمر بوصفه استغلالاً فعليًا. تحقّقوا مما إذا كانت جهتكم، أو مزوّد خدمات مُدارة يعمل لصالحها، يشغّل VeloCloud Orchestrator، واطّلعوا على تنبيه المورّد لمعرفة إجراءات المعالجة. راجعوا من يملك حسابات على المنسّق، فحتى الحسابات منخفضة الصلاحية معنية هنا، وافحصوا السجلات بحثًا عن تغييرات غير متوقعة في الصلاحيات أو مستخدمين جدد بمستوى مشغّل.

ما يجب فعله الآن

1. حدّدوا ما إذا كان VeloCloud Orchestrator منشورًا في بيئتكم أو يُدار نيابةً عنكم من مزوّد خدمة.
2. اطّلعوا على تنبيه Arista بتاريخ 22 أكتوبر وطبّقوا إجراءات المعالجة أو التحديثات التي يحددها.
3. دقّقوا جميع الحسابات على المنسّق، بما فيها حسابات العملاء للقراءة فقط، وأزيلوا غير الضروري منها.
4. راجعوا سجلات المنسّق بحثًا عن رفع صلاحيات غير متوقع أو مستخدمين جدد بمستوى مشغّل.
5. قيّدوا الوصول الشبكي إلى واجهة إدارة المنسّق بمصادر موثوقة قدر الإمكان.
6. أبلغوا عن أي اختراق مؤكد عبر مسار الاستجابة للحوادث، وأشعروا الهيئة الوطنية للأمن السيبراني أو البنك المركزي السعودي وفق التزاماتكم.