

ثغرة حرجية في التحقق من المدخلات في Arista VeloCloud Orchestrator تتطلب تصحيحاً فورياً



ثغرة حرجية في التحقق من المدخلات في النسخ المحلية من Arista VeloCloud Orchestrator قد تسمح لمهاجمين عن بُعد بالوصول إلى وظائف ذات امتيازات عالية والإضرار بسرية وسلامة وتوافر المنصة.

- الثغرة CVE-2026-93952 تؤثر على التثبيتات المحلية لـ Arista VeloCloud Orchestrator بسبب ضعف في التحقق من المدخلات
- قد يستغل مهاجمون عن بُعد الثغرة للوصول إلى وظائف داخلية ذات امتيازات والتأثير على النظام المضيف
- الاستغلال الناجح يهدد سرية وسلامة وتوافر المنصة والبيانات المُدارة
- وكالة CISA توجه المؤسسات لتطبيق حلول البائع أو إيقاف استخدام المنتج في حال عدم توفر التصديحات

نظرة عامة على الثغرة

تحتوي النسخ المحلية من Arista VeloCloud Orchestrator على **ثغرة حرجية في التحقق من المدخلات** مسجلة برقم CVE-2026-93952. قد تمكن هذه الثغرة مهاجمين عن بُعد من الوصول إلى وظائف داخلية ذات امتيازات عالية والتأثير المباشر على النظام المضيف للمنصة. تواجه المؤسسات التي تستخدم VeloCloud Orchestrator لإدارة الشبكات المُعرّفة برمجياً خطر اختراق محتمل لسرية وسلامة وتوافر المنصة والبيانات التي تديرها.

المخاطر على المؤسسات السعودية

يجب على المؤسسات الخاضعة للتنظيم في المملكة والتي تشغل تثبيتات محلية من VeloCloud Orchestrator أن تعامل هذه الثغرة كأولوية عاجلة للمعالجة. يمثل إمكانية الاستغلال عن بُعد والتأثير المحتمل على الوظائف ذات الامتيازات خطراً كبيراً على البنية التحتية لإدارة الشبكات. يجب على المؤسسات المالية ومقدمي الرعاية الصحية ومشغلي البنى التحتية الحيوية الذين يعتمدون على منصات SD-WAN لربط الفروع أو الوصول السحابي تقييم مدى تعرضهم فوراً.

إرشادات المعالجة

توجه وكالة CISA المؤسسات المتأثرة لتطبيق الحلول المقدمة من البائع وفقاً لإرشادات التصحيح القائمة على المخاطر. في حال عدم توفر تصحيحات أو حلول من البائع، يجب على المؤسسات تقييم إيقاف استخدام المنتج المتأثر. يتعين على مالكي الأصول إجراء جرد لنسخ VeloCloud Orchestrator المعرضة للإنترنت وتحديد أولويات المعالجة بناءً على مستوى التعرض والأهمية التشغيلية. يجب على المؤسسات توثيق أنشطة المعالجة والحفاظ على الجاهزية الجنائية وفقاً لإجراءات الاستجابة للحوادث.

ما يجب فعله الآن

1. إجراء جرد فوري لجميع تثبيتات Arista VeloCloud Orchestrator المحلية في مؤسستك
2. تحديد نسخ VeloCloud Orchestrator المعرضة للإنترنت وتقييم أهميتها الحرجة للعمليات التشغيلية
3. التواصل مع Arista Networks للحصول على التصحيحات أو الحلول الخاصة بالثغرة CVE-2026-93952
4. تطبيق حلول البائع وفقاً لإجراءات إدارة التغيير وبروتوكولات الاختبار
5. في حال عدم توفر التصحيحات، تقييم مستوى تحمل المخاطر والنظر في إيقاف الاستخدام أو عزل الأنظمة المتأثرة
6. توثيق جميع أنشطة المعالجة والاحتفاظ بسجلات جنائية وفقاً لمتطلبات الاستجابة للحوادث لدى الهيئة الوطنية للأمن السيبراني