

ثغرة حرجية في Cisco Catalyst SD-WAN Manager تتيح وصول المسؤول دون مصادقة



ثغرة في ترميز النظام الست عشري في Cisco Catalyst SD-WAN Manager تتيح للمهاجمين عن بُعد دون مصادقة الحصول على صلاحيات المسؤول من خلال معالجة خاطئة لترميز URI في طلبات HTTP.

- الثغرة CVE-2026-76504 تؤثر على Cisco Catalyst SD-WAN Manager بخلل حرج في الترميز الست عشري
- يمكن للمهاجمين عن بُعد دون مصادقة استغلال الترميز الخاطئ لـ URI للحصول على صلاحيات المسؤول
- تتبع الثغرة من المعالجة غير الصحيحة لترميز URI في طلبات HTTP
- يجب على المؤسسات تطبيق إجراءات التخفيف من الموزّد فوراً أو إيقاف استخدام المنتج إذا لم تتوفر التحديثات

نظرة عامة على الثغرة

كشفت Cisco عن ثغرة حرجية تحمل الرقم التعريفي **CVE-2026-76504** تؤثر على Cisco Catalyst SD-WAN Manager. يكمن الخلل في طريقة معالجة النظام للترميز الست عشري ضمن طلبات HTTP، وتحديداً في كيفية معالجة ترميز URI. يمكن لمهاجم عن بُعد دون مصادقة استغلال هذه الثغرة للوصول إلى النظام المتأثر بصلاحيات إدارية كاملة، متجاوزاً آليات المصادقة العادية بالكامل.

تتبع خطورة الثغرة من الجمع بين قابلية الاستغلال عن بُعد، وعدم الحاجة إلى مصادقة، والصلاحيات المرتفعة التي يحصل عليها المهاجم عند نجاح الاستغلال. المؤسسات التي تدير بنية SD-WAN التحتية مع واجهات إدارة معرضة للإنترنت تواجه مخاطر فورية.

المخاطر على المؤسسات السعودية

يجب على المؤسسات الخاضعة للرقابة في المملكة والتي تشغل Cisco Catalyst SD-WAN Manager التعامل مع هذا الأمر كحادث ذي أولوية. إن قدرة المهاجمين على الحصول على وصول بمستوى المسؤول دون بيانات اعتماد تخلق تعرضاً لسرقة البيانات، والتلاعب بالشبكة، وانتهاكات محتملة للامتثال بموجب الأطر التنظيمية بما في ذلك ضوابط الهيئة الوطنية للأمن السيبراني ومتطلبات الأمن السيبراني لمؤسسة النقد العربي السعودي.

تتمتع منصات إدارة SD-WAN عادةً برؤية وتحكم في حركة مرور الشبكة واسعة النطاق، مما يجعل اختراقها ذا عواقب خاصة للمؤسسات المالية ومقدمي الرعاية الصحية ومشغلي البنية التحتية الحيوية.

الاستجابة الفورية

يجب تطبيق إجراءات التخفيف من المورّد فوراً وفقاً للنشرات الأمنية من Cisco. يجب على المؤسسات جرد جميع عمليات نشر Cisco Catalyst SD-WAN Manager، وتقييم تعرض واجهات الإدارة للإنترنت، وتحديد أولويات التصحيح بناءً على المخاطر. إذا لم تكن تحديثات المورّد متاحة بعد، ففكر في تجزئة الشبكة، أو قيود الوصول، أو الإيقاف المؤقت للخدمة حتى يمكن نشر إجراءات التخفيف. وثّق جميع الإجراءات لأغراض التدقيق والامتثال.

ما يجب فعله الآن

1. جرد فوري لجميع عمليات نشر Cisco Catalyst SD-WAN Manager في مؤسستك
2. تطبيق التحديثات الأمنية وإجراءات التخفيف المقدمة من المورّد فور توفرها
3. تقييم وتوثيق تعرض جميع واجهات إدارة SD-WAN للإنترنت
4. تنفيذ تجزئة الشبكة وضوابط الوصول لتقييد الوصول إلى واجهة الإدارة للشبكات المؤنوقة فقط
5. إذا لم تكن التحديثات متاحة، ففكر في الإيقاف المؤقت للاستخدام أو عزل الأنظمة المتأثرة حتى يمكن نشر إجراءات التخفيف
6. توثيق جميع إجراءات المعالجة والجدول الزمني لإعداد التقارير التنظيمية للهيئة الوطنية للأمن السيبراني أو مؤسسة النقد أو الجهات الرقابية الأخرى