

## CISA تضيف ثغرة جديدة إلى سجل الثغرات المستغلة المعروفة



أضافت CISA ثغرة جديدة إلى سجل الثغرات المستغلة المعروفة، مما يبرز الحاجة إلى أن تعطي المؤسسات الأولوية لجهود الإصلاح للثغرات عالية المخاطر.

- تتعلق الإضافة الجديدة من CISA بثغرة في Cisco Catalyst SD-WAN Manager.
- الثغرة مستغلة بنشاط وتشكل مخاطر كبيرة.
- يُشجع على اعتماد إدارة الثغرات بناءً على المخاطر.
- الإصلاح السريع للثغرات عالية المخاطر أمر ضروري.
- ستستمر CISA في تحديث السجل بثغرات جديدة.

## نظرة عامة

أضافت CISA مؤخرًا ثغرة جديدة إلى سجل الثغرات المستغلة المعروفة (KEV). تسلط هذه الإضافة الضوء على التهديد المستمر الذي تشكله الثغرات التي يتم استغلالها بنشاط من قبل الجهات الخبيثة.

تؤثر الثغرة المحددة حديثًا على Cisco Catalyst SD-WAN Manager وتُصنف على أنها خطر كبير. يُنصح المؤسسات بأخذ هذا التحديث على محمل الجد والنظر في تداعياته على وضعها الأمني.

## التوصيات

بينما ينطبق التوجيه التشغيلي الملزم (BOD) 26-04 بشكل خاص على وكالات الحكومة الفيدرالية المدنية، تشجع CISA جميع المؤسسات على اعتماد ممارسات مماثلة. إن إعطاء الأولوية لإصلاح الثغرات المدرجة في سجل KEV أمر بالغ الأهمية للحفاظ على الأمن.

يجب على المؤسسات مراجعة أنظمتها بانتظام بحثًا عن الثغرات والتأكد من أنها تطبق التصحيحات على الفور. يعد سجل CISA مصدرًا قيمًا لتحديد الثغرات الحرجة التي تتطلب اهتمامًا فوريًا.

## الخطوات التالية

يجب على المؤسسات في المملكة العربية السعودية النظر في الإجراءات التالية لمعالجة هذه الثغرة الجديدة وتعزيز استراتيجيتها الأمنية العامة:

- إجراء تقييم للمخاطر لتحديد الأنظمة المتأثرة بالثغرة الجديدة.
- إعطاء الأولوية لجهود الإصلاح للثغرات المدرجة في سجل KEV.
- تنفيذ عملية إدارة تصحيحات منتظمة لضمان التحديثات في الوقت المناسب.
- مراقبة سجل KEV الخاص بـ CISA للحصول على تحديثات جديدة وثغرات جديدة.
- تدريب الموظفين على التعرف على محاولات الاستغلال المحتملة والاستجابة لها.

## ما يجب فعله الآن

1. إجراء تقييم للمخاطر لتحديد الأنظمة المتأثرة بالثغرة الجديدة.
2. إعطاء الأولوية لجهود الإصلاح للثغرات المدرجة في سجل KEV.
3. تنفيذ عملية إدارة تصحيحات منتظمة لضمان التحديثات في الوقت المناسب.
4. مراقبة سجل KEV الخاص بـ CISA للحصول على تحديثات جديدة وثغرات جديدة.
5. تدريب الموظفين على التعرف على محاولات الاستغلال المحتملة والاستجابة لها.