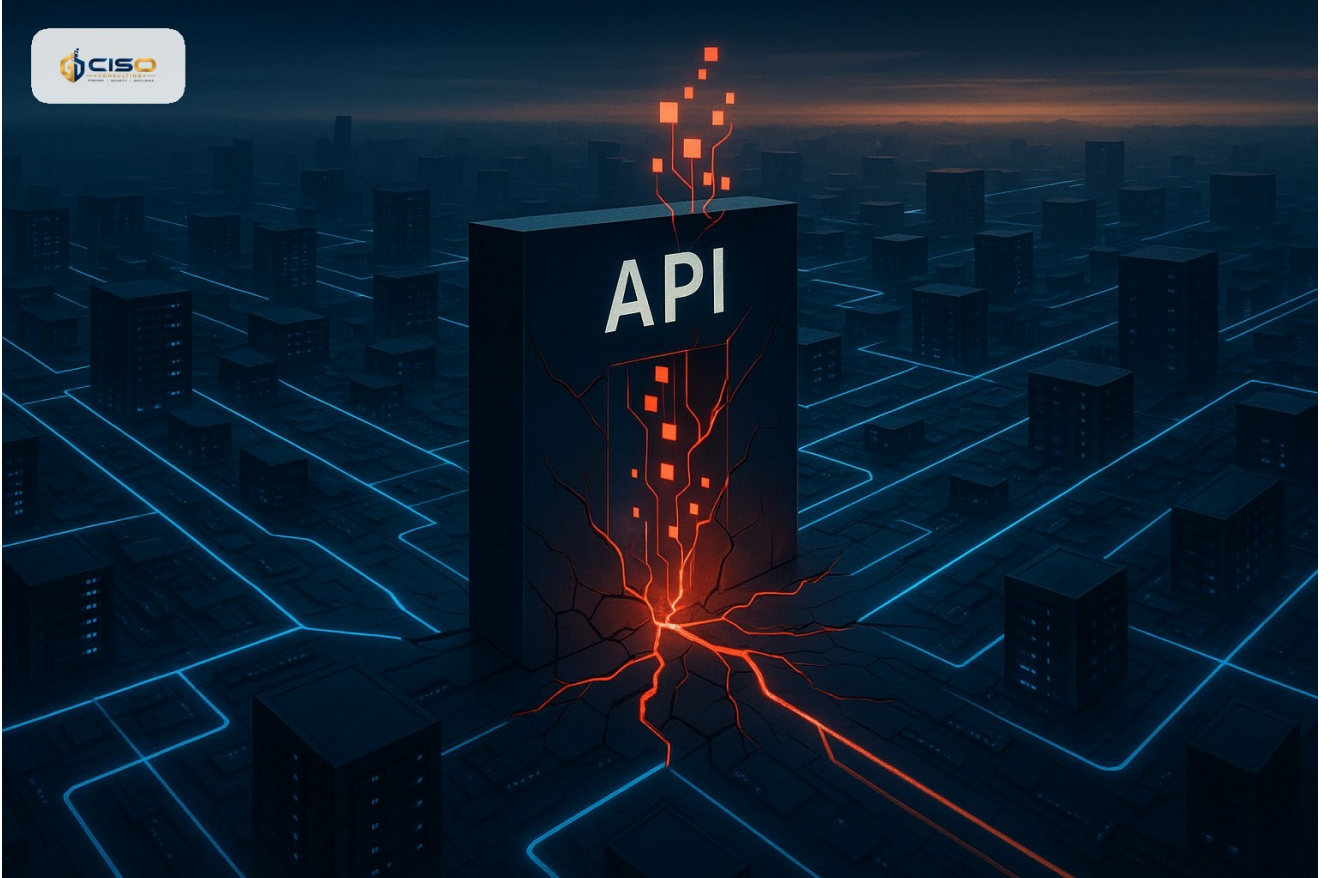


ثغرة اجتياز المسار في منتجات WSO2 API تتيح تنفيذ التعليمات البرمجية عن بُعد



ثغرة اجتياز المسار في منتجات WSO2 للواجهات البرمجية تسمح برفع ملفات غير مقيد وقد تؤدي إلى تنفيذ تعليمات برمجية عن بُعد.

- الثغرة CVE-2026-5430 تؤثر على WSO2 API Control Plane و API Manager و Traffic Manager و Universal Gateway
- عيب اجتياز المسار يسمح برفع ملفات غير مقيد مما يؤدي إلى احتمال تنفيذ تعليمات برمجية عن بُعد
- يجب على المؤسسات تطبيق إجراءات الموزد التخفيفية أو إيقاف استخدام المنتج في حال عدم توفر التحديثات
- الأصول المعرضة للإنترنت تتطلب تقييماً فورياً وأولوية في المعالجة

نظرة عامة على الثغرة

أفصحت WSO2 عن ثغرة اجتياز المسار المتتبع برقم CVE-2026-5430 والتي تؤثر على منتجات متعددة لإدارة الواجهات البرمجية. يؤثر العيب على WSO2 API Control Plane و API Manager و Traffic Manager و Universal Gateway. تسمح الثغرة للمهاجمين برفع ملفات دون قيود، مما يخلق مساراً لتنفيذ تعليمات برمجية عن بُعد على الأنظمة المتأثرة.

تسمح ثغرات اجتياز المسار للجهات الخبيثة بالوصول إلى أدلة وملفات مخزنة خارج هيكل المجلدات المقصود. في هذه الحالة، يتيح الضعف إمكانيات رفع ملفات غير مقيدة يمكن استغلالها لوضع تعليمات برمجية قابلة للتنفيذ على الخوادم المعرضة للخطر، مما يمنح المهاجمين السيطرة على البنية التحتية المتأثرة.

المخاطر على المؤسسات الخاضعة للتنظيم

تواجه المؤسسات التي تشغل منصات WSO2 لإدارة الواجهات البرمجية مخاطر فورية إذا بقيت الأنظمة دون تحديث. عادةً ما تتعامل البنية التحتية لإدارة الواجهات البرمجية مع المصادقة والتفويض وتوجيه البيانات للخدمات الحيوية، مما يجعل اختراقها ذا عواقب خاصة للجهات الخاضعة للتنظيم. قد يؤدي الاستغلال الناجح إلى وصول غير مصرح به للبيانات الحساسة أو تعطيل الخدمات أو الحركة الجانبية داخل شبكات المؤسسة.

يجب على المؤسسات تقييم جرد أصولها لتحديد جميع نشر منتجات WSO2 المتأثرة، مع إيلاء اهتمام خاص للحالات المواجهة للإنترنت. تتطلب التطبيقات المستضافة سحابياً التنسيق مع مزودي الخدمة لضمان تطبيق الإجراءات التخفيفية المناسبة.

إرشادات المعالجة

يجب تطبيق إجراءات المورد التخفيفية فوراً وفقاً لنشرات WSO2 الأمنية. في حال عدم توفر التحديثات أو الإجراءات التخفيفية، يجب على المؤسسات تقييم ما إذا كان استمرار تشغيل المنتجات المتأثرة مقبولاً بالنظر إلى ملف المخاطر، أو ما إذا كان إيقاف الخدمة المؤقت مبرراً حتى يصبح توجيه المورد متاحاً. يجب توثيق جميع أنشطة المعالجة لإثبات الامتثال لأطر الأمن السيبراني المعمول بها والتوقعات التنظيمية.

ما يجب فعله الآن

1. إجراء مسح فوري لجرد الأصول لتحديد جميع نشر WSO2 API Control Plane و API Manager و Traffic و Universal Gateway في بيئتك
2. إعطاء الأولوية لحالات WSO2 المعرضة للإنترنت للتقييم والمعالجة الفورية
3. مراجعة النشرات الأمنية من مورد WSO2 وتطبيق الإجراءات التخفيفية أو التحديثات الموصى بها دون تأخير
4. بالنسبة لخدمات WSO2 المستضافة سحابياً، الاتصال بمزود الخدمة لتأكيد حالة الإجراءات التخفيفية والجدول الزمني
5. في حال عدم توفر إجراءات تخفيفية من المورد، إجراء تقييم للمخاطر لتحديد ما إذا كان إيقاف الخدمة المؤقت مبرراً
6. توثيق جميع أنشطة المعالجة والاحتفاظ بالأدلة لإعداد تقارير الامتثال للهيئة الوطنية للأمن السيبراني أو

مؤسسة النقد العربي السعودي أو الجهات التنظيمية المعنية الأخرى