

ثغرة في التحقق من المدخلات في Citrix NetScaler تتيح تنفيذ أوامر عن بُعد دون مصادقة



تحتوي منتجات Citrix NetScaler ADC و Gateway على ثغرة في التحقق من صحة المدخلات تتيح للمهاجمين غير المصادقين تنفيذ أوامر عشوائية عن بُعد.

- منتجات Citrix NetScaler ADC و NetScaler Gateway متأثرة بثغرة في التحقق من المدخلات تحمل الرقم CVE-2026-88771
- يمكن للمهاجمين غير المصادقين استغلال الثغرة لتنفيذ أوامر عشوائية على الأنظمة المعرضة للخطر
- وجهت CISA الجهات الفيدرالية الأمريكية لتطبيق تدابير المورّد بحلول 30 سبتمبر 2026
- يجب على المؤسسات تقييم مدى تعرض الأصول المتأثرة للإنترنت وتحديد أولويات التصحيح بناءً على المخاطر
- يُطلب إيقاف استخدام المنتج في حال عدم توفر تدابير الحماية من المورّد

نظرة عامة على الثغرة

تحتوي منتجات Citrix NetScaler ADC و NetScaler Gateway على ثغرة حرجية في التحقق من صحة المدخلات تحمل الرقم CVE-2026-88771. تتيح هذه الثغرة للمهاجمين عن بُعد غير المصادقين تنفيذ أوامر عشوائية على الأنظمة المتأثرة دون الحاجة إلى بيانات اعتماد صالحة. تمثل هذه الثغرة تعرضاً كبيراً للمؤسسات التي تعتمد على هذه الحلول المنتشرة على نطاق واسع لتوصيل التطبيقات والوصول الآمن.

أصدرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية إرشادات تطالب الجهات الفيدرالية بتطبيق تدابير الحماية المقدمة من المورد بحلول 30 سبتمبر 2026، وفقاً للتوجيه التشغيلي الملزم 04-26 بشأن تحديد أولويات التحديثات الأمنية بناءً على المخاطر. يشير التوجيه أيضاً إلى متطلبات الفحص الجنائي للأنظمة المتأثرة.

تقييم المخاطر والتعرض

يجب على المؤسسات تقييم أصول NetScaler المعرضة للإنترنت فوراً، حيث تمثل هذه الأصول سطح الهجوم الأعلى خطورة. إن قدرة المهاجمين غير المصادقين على تنفيذ الأوامر عن بُعد تجعل الحالات المواجهة للإنترنت عرضة بشكل خاص للاستغلال. ينبغي للمؤسسات الخاضعة للتنظيم في المملكة تقييم نشر NetScaler لديها مقابل قدرتها على تحمل المخاطر والتزاماتها التنظيمية.

تؤكد إرشادات CISA أنه في حال عدم توفر تدابير الحماية من المورد، يجب على المؤسسات إيقاف استخدام المنتج المتأثر. وهذا يؤكد خطورة الثغرة والخيارات المحدودة للحد من المخاطر بخلاف التصحيحات المقدمة من المورد.

اعتبارات الامتثال

ينبغي للجهات الخاضعة للتنظيم في المملكة والتي تستخدم منتجات NetScaler مواءمة جهود المعالجة مع أطر الهيئة الوطنية للأمن السيبراني والمتطلبات الخاصة بكل قطاع. يُعد التصحيح الفوري للأنظمة المواجهة للإنترنت والجرد الشامل للأصول من المكونات الأساسية لبرامج إدارة الثغرات الفعالة المطلوبة بموجب أطر تنظيمية متعددة.

ما يجب فعله الآن

1. إجراء جرد فوري لجميع حالات Citrix NetScaler ADC و NetScaler Gateway في بيئتك
2. تحديد وتصنيف أنظمة NetScaler المواجهة للإنترنت حسب الأولوية للمعالجة العاجلة
3. الاتصال بدعم Citrix للحصول على تدابير الحماية الأمنية وتطبيقها للثغرة CVE-2026-88771
4. تطبيق مراقبة وتسجيل معززين لجميع أنظمة NetScaler حتى يتم تطبيق التصحيحات
5. إعداد خطط طوارئ لإيقاف استخدام NetScaler في حال عدم توفر تدابير الحماية من المورد
6. توثيق أنشطة المعالجة والجدول الزمنية لإعداد تقارير الامتثال للهيئة الوطنية للأمن السيبراني والجهات التنظيمية القطاعية