

# تحذير من وكالة الأمن السيبراني الأمريكية بشأن ثغرة في ذاكرة Citrix NetScaler ADC وGateway

أصدرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية تنبيهاً بشأن الثغرة CVE-2026-88779 في منتجات Gateway وCitrix NetScaler ADC والتي قد تؤدي إلى تعطيل الخدمة.

- تؤثر الثغرة CVE-2026-88779 على Citrix NetScaler Gateway وCitrix NetScaler ADC بسبب قيود غير صحيحة على ذاكرة التخزين المؤقت
- قد تمكن الثغرة من شن هجمات حجب الخدمة على الأنظمة المتأثرة
- توجه الوكالة الأمريكية المؤسسات لتطبيق إجراءات الحماية من المورد وتقييم مدى تعرض الأصول للإنترنت
- يجب على المؤسسات اتباع إرشادات التصحيح القائمة على المخاطر أو إيقاف استخدام المنتج في حال عدم توفر الحلول

## نظرة عامة على الثغرة

أصدرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية تنبيهاً يتعلق بالثغرة **CVE-2026-88779** التي تؤثر على Citrix NetScaler ADC (المعروف سابقاً باسم Citrix ADC) وCitrix NetScaler Gateway (المعروف سابقاً باسم Citrix Gateway). تتمثل الثغرة في قيود غير صحيحة على العمليات ضمن حدود ذاكرة التخزين المؤقت، وهي حالة يمكن استغلالها للتسبب في حجب الخدمة على الأنظمة المعرضة للخطر.

## الإجراءات المطلوبة وإرشادات الامتثال

توجه الوكالة الأمريكية المؤسسات لتطبيق إجراءات الحماية وفقاً لتعليمات المورد. يشير التنبيه إلى إرشادات BOD 26-04 الخاصة بالوكالة حول تحديد أولويات التحديثات الأمنية بناءً على المخاطر، بالإضافة إلى متطلبات الفرز الجنائي. يُطلب من أصحاب المصلحة تقييم مدى تعرض كل أصل متأثر للإنترنت والتأكد من الالتزام بإرشادات التصحيح الواردة في التوجيه التشغيلي الملزم. في حال عدم توفر إجراءات الحماية، يجب على المؤسسات اتباع الإرشادات المعمول بها للخدمات السحابية أو إيقاف استخدام المنتج.

## التداعيات على المؤسسات السعودية

يتعين على المؤسسات الخاضعة للتنظيم في المملكة والتي تستخدم منتجات Citrix NetScaler في أدوار توصيل التطبيقات أو الوصول الآمن عن بُعد مراجعة مخزوناتهما فوراً. نظراً لاحتمال تعطل الخدمة، يجب على المؤسسات تقييم ما إذا كانت الأنظمة المتأثرة متصلة بالإنترنت وتحديد أولويات المعالجة وفقاً لذلك. يُعد التنسيق مع الموردين

وفرق الأمن الداخلية أمراً ضرورياً للحفاظ على المرونة التشغيلية أثناء معالجة هذه الثغرة بما يتماشى مع الأطر القائمة على المخاطر.

## ما يجب فعله الآن

1. حدد جميع عمليات نشر Citrix NetScaler ADC و Gateway في بيئتك ووثّق إصداراتها
2. قيّم ما إذا كانت الأنظمة المتأثرة متصلة بالإنترنت أو معرضة لشبكات غير موثوقة
3. تواصل مع Citrix أو الموزع المعتمد للحصول على إرشادات الحماية والتوصيات الخاصة بالموّرد
4. طبّق إجراءات الحماية أو التوصيات الموصى بها من الموزّرد وفقاً لعمليات إدارة التغيير وتقييم المخاطر لديك
5. في حال عدم توفر إجراءات الحماية، قيّم الضوابط البديلة أو أوقف استخدام المنتجات المتأثرة حتى يصبح الإصدار ممكناً
6. وثّق إجراءات المعالجة والجدول الزمنية لأغراض المراجعة والامتثال بما يتماشى مع متطلبات الهيئة الوطنية للأمن السيبراني ومؤسسة النقد العربي السعودي