ثغرات حرجة في Citrix NetScaler ADC وGateway: استغلال فعلي لثغرتين من نوع تنفيذ الأوامر عن بُعد



أصدرت Citrix إصلاحات لثماني ثغرات في NetScaler ADC وGateway المُدارة من العميل، بينها ثغرتان حرجتان لتنفيذ الأوامر عن بُعد مستغلتان فعليًا. وتوصي CERT-EU بالتحديث الفوري وفحص الاختراق.

- تشمل نشرة Citrix الصادرة في 27 سبتمبر 2026 ثماني ثغرات في NetScaler ADC وNetScaler Gateway المُدارة من العميل.
- الثغرة CVE-2026-88771 (CVSS 9.5) تتيح تنفيذ أوامر عن بُعد دون مصادقة وبلا شروط مسبقة، فتمسّ جميع النشرات، وهي مستغلة فعليًا.
- الثغرة CVE-2026-88772 (CVSS 9.5) فيض في الذاكرة قد يؤدي إلى RCE أو DoS عند تفعيل DTLS (الافتراضي في VPN vServer)، وهي مستغلة أيضًا.
- تشمل الإصدارات المتأثرة 13.1 قبل 13.1-64.23 و14.1 قبل 14.1-73.37، ونسخ FIPS وNDcPP،

ونشرات Secure Private Access Hybrid التي تستخدم NetScaler.

- توصي CERT-EU بالتحديث الفوري وإجراء تقييم اختراق للأجهزة المكشوفة على الإنترنت.

ما الذي حدث

نشرت Citrix في 27 سبتمبر 2026 نشرة أمنية تعالج ثماني ثغرات في NetScaler ADC وNetScaler Gateway المُدارة من العميل. ثغرتان منها حرجتان وتتيحان تنفيذ أوامر عن بُعد دون مصادقة، وقد أكدت Citrix استغلالهما فعليًا. وأصدرت CERT-EU تنبيهًا يوصي بالتحديث العاجل.

الصورة التقنية

الثغرة **CVE-2026-88771** (CVSS 9.5) ناتجة عن ضعف التحقق من المدخلات، ولا تتطلب شروطًا مسبقة، ولذلك تتعرض لها جميع نشرات NetScaler ADC وGateway. أما **CVE-2026-88772** (CVSS 9.5) فهي فيض في الذاكرة قد يقود إلى RCE أو حجب الخدمة عند تفعيل DTLS، وهو الإعداد الافتراضي في VPN vServer.

وتعتمد بقية الثغرات على الإعدادات. فـ CVE-2026-88773 (CVSS 9.3) تهريب طلبات HTTP، وCVE-2026-88774 (CVSS 7.0) تجاوز للسياسات، وكلاهما مرتبط بتعبيرات سياسات قائمة على HTTP URL. أما CVE-2026-88775 وCVE-2026-88776 (CVSS 8.8) CVE-2026-88777 لكل منها) فهي فيض ذاكرة مرتبط بإعدادات vServer أو بروتوكولات محددة، وCVE-2026-88778 (CVSS 8.8) تنبؤ برقم التسلسل الابتدائي TCP ISN عند تعطيل Enhanced ISN Generation.

الإصدارات المتأثرة

تتأثر إصدارات NetScaler ADC وGateway من 13.1 قبل 13.1-64.23 ومن 14.1 قبل 14.1-73.37، وكذلك ADC FIPS 14.1 قبل 14.1-73.37 FIPS، وADC FIPS و13.1 NDcPP قبل 13.1-37.279. كما يجب ترقية نشرات Secure Private Access Hybrid التي تستخدم NetScaler. وتنطبق النشرة على النشرات المُدارة من العميل فقط.

توصي CERT-EU بتحديث الأجهزة المتأثرة فورًا، وتفعيل Enhanced ISN Generation حيث تكون إعدادات TCP مفعلة، وإجراء تقييم اختراق لأي جهاز مكشوف على الإنترنت يعمل بإصدار متأثر.

ما يجب فعله الآن

1. احصر جميع أجهزة NetScaler ADC وGateway المُدارة من المؤسسة، بما فيها FIPS وNDcPP ونشرات Secure Private Access Hybrid، وقارن إصداراتها بالإصدارات المصححة.
2. رقِّ الأجهزة المتأثرة إلى الإصدارات المصححة فورًا، مع إعطاء الأولوية للأنظمة المكشوفة على الإنترنت.
3. أجرِ تقييم اختراق لكل جهاز مكشوف على الإنترنت كان يعمل بإصدار متأثر، لأن الاستغلال مؤكد.
4. فعّل Enhanced ISN Generation أينما كانت إعدادات TCP مفعلة.
5. راجع خطوات التحقق من الشروط المسبقة في نشرة Citrix (DTLS وتعبيرات سياسات HTTP URL وأنواع vServer) لتحديد مدى التعرض.
6. وثّق الحدث والاستجابة ضمن إجراءات إدارة الحوادث والثغرات، وأبلغ الهيئة الوطنية للأمن السيبراني أو

البنك المركزي السعودي (ساما) متى اقتضت التزاماتكم ذلك.