

إشعار حول ثغرات Citrix NetScaler



حددت NCSC ثغرات في Citrix NetScaler ADC و Gateway، مع وجود ثغرتين يتم استغلالهما بنشاط. يجب على المؤسسات اتخاذ إجراءات فورية للتخفيف من المخاطر.

- تم تحديد ثماني ثغرات في Citrix NetScaler ADC و Gateway.
- يتم استغلال ثغرتين بنشاط.
- يجب على المؤسسات مراجعة نشرة أمان Citrix.
- يوصى بعزل الأنظمة المتأثرة وتحديثها على الفور.
- يجب تنفيذ المراقبة المستمرة وأنشطة البحث عن التهديدات.

نظرة عامة

أصدرت المركز الوطني للأمن السيبراني (NCSC) تحذيرًا بشأن ثغرات في Citrix NetScaler و Citrix NetScaler ADC.

Gateway. تشكل هذه الثغرات مخاطر كبيرة، خاصة وأن اثنتين منها تم تأكيد استغلالهما بنشاط من قبل المهاجمين.

الأنظمة المتأثرة

يجب على المؤسسات التي تستخدم Citrix NetScaler ADC أو Gateway أن تكون على دراية بأن إصدارات معينة معرضة للخطر. من الضروري تقييم ما إذا كانت أنظمتك تقع ضمن الفئات المتأثرة واتخاذ الإجراءات المناسبة للتخفيف من المخاطر المحتملة.

الإجراءات الموصى بها

لحماية مؤسستك، ضع في اعتبارك اتخاذ الإجراءات التالية:

- مراجعة نشرة أمان Citrix للحصول على معلومات مفصلة حول الثغرات.
- عزل أي أنظمة متأثرة واستبدالها بإصدارات محدثة إذا كان ذلك ممكناً.
- التحقيق في علامات الاختراق باستخدام مؤشرات الاختراق (IoCs) المقدمة من Citrix.
- تثبيت آخر التحديثات كما هو موصى به من قبل Citrix لسد الثغرات.
- مراقبة التهديدات بشكل مستمر واستخدام أدوات مثل NetScaler Console File Integrity Monitoring لاكتشاف التغييرات غير المصرح بها.

ما يجب فعله الآن

1. مراجعة نشرة أمان Citrix.
2. عزل الأنظمة المتأثرة والنظر في استبدالها.
3. التحقيق في علامات الاختراق باستخدام مؤشرات الاختراق.
4. تثبيت آخر التحديثات من Citrix.
5. مراقبة التهديدات بشكل مستمر.