

الكشف عن ثغرات حرجية متعددة في منتجات Adobe وNVIDIA والبنية التحتية لنظام أسماء النطاقات



كشف باحثون أمنيون عن أكثر من 27 ثغرة هذا الأسبوع، تشمل ثغرات تنفيذ تعليمات برمجية عن بُعد في منتجات Adobe، ومشاكل الهروب من الحاويات في برمجيات NVIDIA، وتقنيات سرقة محافظ العملات المشفرة عبر نظام أسماء النطاقات.

- منتجات Adobe متأثرة بثغرات تنفيذ تعليمات برمجية عن بُعد تتطلب تصحيحاً فورياً
- برمجيات حاويات NVIDIA تحتوي على ثغرات هروب تسمح للمهاجمين بكسر العزل الأمني
- استغلال البنية التحتية لنظام أسماء النطاقات لسرقة محافظ العملات المشفرة عبر التلاعب بالنطاقات
- تحديد تقنيات أبواب خلفية ذاتية الإصلاح تستعيد وصول المهاجم تلقائياً بعد الإزالة
- الكشف عن أكثر من 27 ثغرة متميزة تؤثر على برمجيات المؤسسات والبنية التحتية

مشهد الثغرات الأمنية

كشف باحثون أمنيون عن موجة كبيرة من الثغرات تؤثر على برمجيات وبنية تحتية مؤسسية واسعة الانتشار. تشمل الإفصاحات ثغرات تنفيذ تعليمات برمجية عن بُعد في منتجات Adobe، وثغرات هروب من الحاويات في برمجيات NVIDIA، وتقنيات هجوم مبتكرة تستغل البنية التحتية لنظام أسماء النطاقات لسرقة محافظ العملات المشفرة. يؤكد اتساع نطاق الأنظمة المتأثرة على تعقيد سطح الهجوم الحديث الذي تواجهه المؤسسات الخاضعة للتنظيم.

تمكّن ثغرات Adobe المهاجمين من تنفيذ تعليمات برمجية عشوائية عن بُعد، مما يشكل خطراً فورياً على المؤسسات التي تستخدم المنتجات المتأثرة. وُجد أن برمجيات حاويات NVIDIA تحتوي على ثغرات هروب تسمح للمهاجمين بالخروج من البيئات المعزولة، مما قد يعرض الأنظمة المضيفة للخطر. بشكل منفصل، حدد الباحثون أساليب هجوم قائمة على نظام أسماء النطاقات تتلاعب بحل النطاقات لإعادة توجيه معاملات العملات المشفرة.

أنماط التهديدات الناشئة

من بين التهديدات المكشوفة، حددت فرق الأمن السيبراني تقنيات أبواب خلفية ذاتية الإصلاح تستعيد وصول المهاجم تلقائياً بعد أن تزيل الإجراءات الدفاعية الاختراقات الأولية. تمثل آلية الاستمرارية هذه تطوراً في أساليب المهاجمين، مما يتطلب من المدافعين معالجة ليس فقط الإصابات الأولية بل أيضاً قدرات الاستعادة الآلية.

تمتد مجموعة أكثر من 27 ثغرة مكشوفة هذا الأسبوع عبر موردين وفئات منتجات متعددة، مؤثرة على برمجيات التطبيقات ومكونات البنية التحتية. تواجه المؤسسات التي تعتمد على أنظمة إدارة الهوية والوصول تعرضاً خاصاً، حيث يمكن لأخطاء صغيرة في تكوين الصلاحيات أن تمكّن من سرقة بيانات كبيرة. يستمر نمط الثغرات القديمة في إيجاد ضحايا جدد، حيث يعيد المهاجمون استخدام أدوات مألوفة لسلاسل هجوم جديدة.

المخاطر على المؤسسات السعودية

ينبغي على الجهات الخاضعة للتنظيم في المملكة إعطاء الأولوية لتصحيح منتجات Adobe و NVIDIA حيثما كانت منشورة. تستحق ضوابط أمن نظام أسماء النطاقات مراجعة فورية، خاصة للمؤسسات التي تتعامل مع الأصول الرقمية أو معاملات العملات المشفرة. تتطلب تكوينات أمن الحاويات التحقق لضمان العزل المناسب بين أعمال العمل والأنظمة المضيفة.

ما يجب فعله الآن

1. جرد جميع منتجات Adobe و NVIDIA المنشورة في المؤسسة وتطبيق التصحيحات الأمنية من الموردين فوراً
2. مراجعة ضوابط أمن نظام أسماء النطاقات وتنفيذ التحقق من DNSSEC لمنع هجمات اختطاف النطاقات
3. تدقيق تكوينات بيئة تشغيل الحاويات للتحقق من العزل المناسب وتطبيق تحديثات NVIDIA الأمنية حيثما تُستخدم منصات الحاويات
4. فحص الأنظمة بحثاً عن آليات الاستمرارية والأبواب الخلفية ذاتية الإصلاح باستخدام مؤشرات استخبارات التهديدات المحدثة
5. مراجعة سياسات إدارة الهوية والوصول لتحديد ومعالجة الصلاحيات الزائدة التي قد تمكّن من تصعيد الامتيازات

6. تحديث إجراءات الاستجابة للحوادث لمعالجة تقنيات استعادة المهاجم الآلية وضمان القضاء الكامل على التهديدات