ثغرتان حرجتان في NGINX باسم «nginx2root» تتيحان تنفيذ تعليمات برمجية عن بُعد على خوادم الويب



ثغرتان حرجتان في NGINX تُعرفان باسم nginx2root تتيحان لمهاجم غير موثّق تنفيذ تعليمات برمجية عن بُعد، وقد بيّن باحثون إمكانية ربطهما بثغرة في نواة لينكس للحصول على صلاحيات الجذر.

- ثغرتان حرجتان في NGINX مجمّعتان تحت اسم nginx2root.
- يمكن لمهاجم غير موثّق تنفيذ تعليمات برمجية عن بُعد على الخوادم المتأثرة.
- أظهر الباحثون إمكانية ربط الثغرتين بثغرة في نواة لينكس للوصول إلى صلاحيات الجذر.
- المقتطف المتاح لا يذكر أرقام CVE ولا الإصدارات المتأثرة ولا تفاصيل التصحيح.

ما الذي ورد في التقرير

أفاد موقع BleepingComputer بوجود ثغرتين حرجتين في NGINX تُعرفان معًا باسم «nginx2root». ووفق التقرير،

تتيح الثغرتان لمهاجم دون أي مصادقة تنفيذ تعليمات برمجية عن بُعد على خادم ويب معرّض للخطر.

كما أظهر باحثون أن بالإمكان ربط الثغرتين بثغرة في نواة لينكس، بما ينقل المهاجم من تنفيذ التعليمات عن بُعد إلى صلاحيات الجذر على الخادم.

ما الذي لم يتضح بعد

لا يتضمن المقتطف المتاح أرقام CVE ولا إصدارات NGINX المتأثرة ولا الإصدارات المعالَجة ولا أي دليل على استغلال فعلي. لذا ينبغي عدم افتراض التعرّض أو السلامة قبل مراجعة نشرات المورّد والمشروع مباشرة.

لماذا يهم المؤسسات المنظَّمة

يُستخدم NGINX عادةً كخادم ويب أو وكيل عكسي أو موزّع أحمال، وغالبًا على حافة الخدمات المتاحة عبر الإنترنت. وثغرة لا تتطلب بيانات اعتماد ويمكن ربطها بالوصول إلى صلاحيات الجذر ترفع أثر اختراق أي خادم مكشوف، ما يستدعي معالجة سريعة ومنظمة دون هلع.

والخطوة الأولى المناسبة هي تحديد أماكن تشغيل NGINX في بيئتكم، بما في ذلك النسخ المضمّنة أو داخل الحاويات، وأيّها متاح من الإنترنت. ثم تُطبَّق الإصلاحات عبر إجراء التغيير الطارئ المعتمد فور صدور الإرشادات الرسمية.

ما يجب فعله الآن

1. حصر جميع نسخ NGINX بما فيها الحاويات والأجهزة والنسخ المضمّنة، وتحديد المتاح منها عبر الإنترنت.
2. مراجعة النشرات الرسمية لـ NGINX لمعرفة أرقام CVE والإصدارات المتأثرة والإصلاحات، وجدولة التصحيح عبر إجراء التغيير الطارئ.
3. التحقق من حالة تحديثات نواة لينكس على الخوادم التي تشغّل NGINX، لأن سلسلة الاستغلال المعروضة تعتمد على ثغرة في النواة.
4. تعزيز مراقبة خوادم NGINX المكشوفة للإنترنت لرصد الطلبات غير المعتادة والعمليات الجديدة وتغيّر الصلاحيات.
5. إذا تعذّر التصحيح فورًا، النظر في ضوابط تعويضية مؤقتة مثل تقييد الوصول عبر جدار حماية تطبيقات الويب أو قواعد الشبكة، وفق توجيهات المورّد.