Check Point تصدر إصلاحات طارئة لثغرة يوم الصفر المستغلة للحصول على صلاحيات الجذر



أصدرت Check Point إصلاحات طارئة لثغرة عالية الخطورة يستغلها المهاجمون منذ أواخر أكتوبر للحصول على صلاحيات الجذر والاحتفاظ بوجودهم في الأجهزة المتأثرة.

- أصدرت Check Point Software إصلاحات طارئة لثغرة يوم صفر عالية الخطورة.
- يستغل المهاجمون الثغرة منذ أواخر أكتوبر.
- يتيح الاستغلال الناجح الحصول على صلاحيات الجذر في الأجهزة الضعيفة.
- استخدم المهاجمون الثغرة أيضاً لترسيخ وجودهم في الأجهزة المتأثرة.

ما الذي حدث

أصدرت Check Point Software إصلاحات طارئة لثغرة يوم صفر عالية الخطورة. ووفق التقرير، يستغل المهاجمون

الثغرة منذ أواخر أكتوبر للحصول على صلاحيات الجذر وترسيخ وجودهم في الأجهزة الضعيفة.

ولا يذكر المقتطف المتاح المنتجات أو الإصدارات المتأثرة، ولا يورد رقم CVE. لذا ينبغي الرجوع إلى نشرة Check Point الرسمية لمعرفة هذه التفاصيل.

أهمية الخبر

تمنح صلاحيات الجذر المهاجم سيطرة كاملة على الجهاز، ويعني ترسيخ الوجود أن الوصول قد يبقى بعد إعادة التشغيل أو التغييرات الروتينية. وبما أن الاستغلال بدأ منذ أواخر أكتوبر، فقد يكون أي جهاز كان مكشوفاً خلال تلك الفترة مخترقاً بالفعل، وبالتالي قد لا يكفي تثبيت الإصلاح وحده.

النهج المقترح

على فرق الأمن التأكد سريعاً مما إذا كانت أجهزة Check Point ضمن النطاق المتأثر في بيئتها، ثم تطبيق الإصلاحات الطارئة من الشركة، ومراجعة تلك الأجهزة بحثاً عن مؤشرات اختراق سابق. وينبغي توثيق النتائج والقرارات ضمن إجراءات إدارة الثغرات والحوادث المعتادة.

ما يجب فعله الآن

1. حصر جميع أجهزة Check Point في بيئتكم ومطابقتها مع نشرة الشركة.
2. تطبيق الإصلاحات الطارئة على الأجهزة المتأثرة بأولوية عالية وفق إجراءات التغيير الطارئ.
3. فحص الأجهزة المتأثرة بحثاً عن مؤشرات اختراق منذ أواخر أكتوبر، مثل حسابات أو عمليات أو تغييرات إعدادات غير متوقعة.
4. رفع أي اشتباه باختراق عبر مسار الاستجابة للحوادث، وإبلاغ الجهات المختصة بحسب الالتزامات المطبقة.
5. توثيق تقييم التعرض والمعالجة في سجل إدارة الثغرات.