تقرير: استغلال بوابات Check Point عبر PHP2Shell لنشر برمجية مسح تستهدف VMware ESXi



أفاد موقع BleepingComputer باختراق بوابات Check Point عبر PHP2Shell لنشر برمجية مسح تستهدف VMware ESXi. لم يكن سوى العنوان مقروءاً، لذا يُنصح بالتحقق من التفاصيل لدى الشركة المصنّعة.

- أفاد BleepingComputer باختراق بوابات Check Point باستخدام أداة تُعرف باسم PHP2Shell.
- الهدف النهائي المذكور هو نشر برمجية مسح (wiper) ضد VMware ESXi.
- نص المقال لم يكن مقروءاً لدينا، لذا فالتفاصيل الفنية والإصدارات المتأثرة ونطاق الحادثة غير مؤكدة.
- تُعد البوابات وبيئات المحاكاة الافتراضية من الأصول عالية الأهمية للجهات المنظمة.

ما الذي ورد في التقرير

نشر موقع BleepingComputer تقريراً بعنوان «اختراق بوابات Check Point عبر PHP2Shell لنشر برمجية مسح تستهدف VMware ESXi». وبحسب العنوان، تمكّن مهاجمون من اختراق بوابات Check Point باستخدام PHP2Shell، ثم استخدموا هذا الوصول لنشر برمجية مسح (wiper) تستهدف VMware ESXi.

ما لم نتمكن من تأكيده

لم يكن نص المقال الأصلي مقروءاً عند إعداد هذا الخبر. لذلك لا يمكننا تحديد المنتجات أو الإصدارات المتأثرة، ولا طريقة الوصول إلى البوابات، ولا الجهة المنفذة، ولا عدد الجهات المتضررة، ولا وجود تحديث أو رقم CVE. ولم نملأ هذه الفجوات بافتراضات. يُرجى الرجوع إلى المقال الأصلي وإلى نشرات Check Point وVMware (Broadcom) مباشرة.

لماذا يهم ذلك

تتعرض بوابات الحدود للشبكة بحكم وظيفتها، وغالباً ما تستضيف خوادم ESXi أنظمة افتراضية حرجة للأعمال. وإذا تم الأمر كما يشير العنوان، فإن أداة تدميرية تستهدف طبقة المحاكاة الافتراضية تهدد توافر الخدمة وقدرة الاستعادة، لا السرية فقط. لذا تتساوى جاهزية الاستعادة في أهميتها مع التحديثات الأمنية.

الاستجابة المتزنة هي التأكد من مدى تعرضكم، ومراجعة إرشادات الشركات المصنّعة، والتحقق من أن النسخ الاحتياطية والفصل الشبكي كفيلان بالصمود عند اختراق بوابة. ولا حاجة لإجراءات متعجلة قبل صدور تفاصيل رسمية.

ما يجب فعله الآن

1. حصر جميع بوابات Check Point لديكم وتأكيد المسؤولين عنها والإصدارات ومدى إتاحة واجهات الإدارة.
2. متابعة النشرات الأمنية الصادرة عن Check Point وVMware (Broadcom) وتطبيق التوصيات فور صدورها.
3. مراجعة سجلات البوابات وخوادم ESXi بحثاً عن نشاط إداري غير معتاد أو ملفات غير متوقعة، ورفع أي ملاحظات إلى مركز العمليات الأمنية.
4. التحقق من أن النسخ الاحتياطية لـ ESXi معزولة أو غير قابلة للتعديل، ومن نجاح اختبار استعادة حديث.
5. التأكد من فصل واجهات إدارة ESXi عن البوابات وعدم إمكانية الوصول إليها من شبكات غير موثوقة.
6. تحديث خطط الاستجابة للحوادث واستمرارية الأعمال بسيناريو هجوم تدميري على البنية الافتراضية.