استهداف بوابات Check Point غير المحدّثة عبر ثغرات PHP2Shell لنشر الباب الخلفي TSGA



أفادت Check Point بأن جهة مجهولة تستغل ثغرات PHP2Shell في بوابات Security Gateways غير المحدّثة، ثم ثغرة رفع صلاحيات في Gaia OS، لنشر الباب الخلفي TSGA. بدأ النشاط في 30 أكتوبر 2026.

- يستهدف المهاجم بوابات Check Point Security Gateways غير المحدّثة للحصول على وصول أولي عبر ثغرات PHP2Shell.
- يُستغل بعدها خلل سبق الإبلاغ عنه لرفع الصلاحيات محليًا في Gaia OS لنشر الباب الخلفي TSGA.
- تذكر Check Point أن النشاط بدأ في 30 أكتوبر 2026 واستهدف أولاً جهات إسرائيلية.
- رُصدت موجة لاحقة أوسع، ويشير العنوان كذلك إلى حذف ملفات ESXi.
- لم تُحدَّد هوية الجهة المهاجمة.

نشرت Check Point تفاصيل حملة اختراق تستهدف فيها جهة مجهولة بوابات Security Gateways التي لم تُحدَّث. يتم الحصول على الوصول الأولي عبر ثغرات PHP2Shell، ثم يستغل المهاجم ثغرة رفع صلاحيات محلية سبق الإبلاغ عنها في Gaia OS لتثبيت باب خلفي يسمى TSGA.

ما هو معروف

وفق Check Point، بدأ النشاط في 30 أكتوبر 2026 واستهدف في البداية جهات إسرائيلية، ثم رُصدت موجة لاحقة أوسع. ويذكر عنوان المصدر أيضًا حذف ملفات ESXi، لكن المقتطف المتاح لا يوضح كيف حدث ذلك أو في أي بيئات، لذا لا نبني استنتاجات على هذه النقطة.

لا يتضمن المقتطف أرقام CVE ولا إصدارات التحديثات ولا مؤشرات الاختراق، ويُرجع إليها في نشرة Check Point نفسها.

أهمية الأمر للجهات في المملكة

تقع بوابات الأمان على حدود الشبكة وتُعد مكونات موثوقة. وإذا اختُرقت البوابة منحت المهاجم موقعًا قويًا، كما أن الإشارة إلى حذف ملفات ESXi تدل على احتمال التأثير في البنية الافتراضية. وعلى الجهات التي تشغّل بوابات Check Point اعتبار ذلك دافعًا للتحقق من حالة التحديثات، دون داعٍ للهلع.

النهج الموصى به

حدّدوا البوابات المستخدمة، وقارنوها بالإصلاحات التي نشرتها Check Point، وراجعوا النشاط الأخير بحثًا عن أي أثر للباب الخلفي TSGA، ضمن إجراءات التغيير والاستجابة للحوادث المعتمدة.

ما يجب فعله الآن

1. حصر جميع بوابات Check Point Security Gateways مع إصدارات Gaia OS.
2. تطبيق الإصلاحات التي نشرتها Check Point لثغرات PHP2Shell ولثغرة رفع الصلاحيات في Gaia OS.
3. البحث عن مؤشرات TSGA وفق إرشادات Check Point، ومراجعة سجلات البوابات منذ أواخر أكتوبر 2026.
4. التأكد من حداثة النسخ الاحتياطية لخوادم ESXi وعزلها أو عدم قابليتها للتعديل وإمكانية استعادتها.
5. تقييد الوصول الإداري إلى البوابات وإحاطة فريق الاستجابة للحوادث بهذه الحملة.