حملة GT13 تخترق خوادم إدارة Check Point لدى 22 جهة



رصدت GreyNoise حملة مستمرة باسم GT13 اخترقت 24 خادم إدارة أمنية من Check Point لدى 22 جهة في 17 دولة، مستغلةً ثغرة تجاوز المصادقة CVE-2026-16232 التي أُعلن عنها في يوليو.

- تأثرت 22 جهة في 17 دولة، منها جهات حكومية ومالية وشركات طاقة ونقل وتعدين وتصنيع.
- استُغلت الثغرة CVE-2026-16232 وهي تجاوز مصادقة في SmartConsole يمنح صلاحيات المسؤول، وكانت Check Point قد أعلنت عنها في يوليو كثغرة مستغلة فعلياً.
- شملت الأنشطة سرقة قواعد بيانات جدران الحماية وبيانات الاعتماد والإعدادات وملفات جهة إصدار الشهادات الداخلية، وإلغاء تحميل سياسات الأمان.
- فقدت GreyNoise الرؤية في 2 نوفمبر لكنها ترجّح استمرار الحملة، وقد شاركت مؤشرات الاختراق.
- تؤكد Check Point أن الثغرة والحمايات ليست جديدة وأن الاستغلال يعتمد على تعديل لوحدة Metasploit العامة.

وصفت شركة استخبارات التهديدات GreyNoise حملة مستمرة تتتبعها باسم GT13، اخترق فيها المهاجمون 24 خادماً لإدارة الأمن من Check Point تعود إلى 22 جهة. تتوزع الجهات على 17 دولة دون مؤشر واضح على استهداف محدد، وتشمل جهات حكومية ومزودي خدمات مالية وشركات في قطاعات الطاقة والنقل والتعدين والتصنيع.

ما تم رصده

أكدت GreyNoise وجود النشاط بين 17 أكتوبر و2 نوفمبر حين انتهت قدرتها على الرصد، وترجّح استمرار الحملة لأن المهاجم ما زال يحتفظ بالوصول. وخلال مراحل ما بعد الاختراق رصدت استغلال **CVE-2026-16232**، وهي ثغرة تجاوز مصادقة في Check Point SmartConsole تتيح للمهاجم الحصول على رمز دخول والمصادقة بصلاحيات المسؤول. ولم تتمكن الشركة من تحديد وقت الاختراق الأولي للخوادم أو أسلوبه.

شملت الإجراءات المسجلة سرقة قواعد بيانات جدران الحماية وبيانات الاعتماد والإعدادات وملفات جهة إصدار الشهادات الداخلية، وإنشاء شهادة جديدة في إحدى البيئات، وإلغاء تحميل سياسات الأمان بما يعطّل حماية الجدار فعلياً، إضافة إلى استطلاع الشبكة الداخلية ومحاولات الحركة الجانبية. كما حاول المهاجمون استهداف منتجات أخرى منها Citrix NetScaler وIvanti وVMware vCenter وMicrosoft Exchange وNetlogon.

موقف المورّد

تفيد Check Point بأن الثغرة أُعلن عنها علناً في يوليو 2026 مع الإشارة إلى رصد استغلالها فعلياً، وبالتالي فهي والحمايات المتاحة ليست جديدة، وأن المهاجمين استخدموا تعديلًا على وحدة Metasploit العامة. وقد أبلغت GreyNoise شركاء حكوميين وفرق CERT ونشرت مؤشرات الاختراق. وتقدّر أن أداة هجومية مدعومة بالذكاء الاصطناعي ربما استُخدمت، لكن ذلك غير مؤكد.

الدلالات

اختراق خادم الإدارة قد يكشف السياسات وبيانات الاعتماد وثقة الشهادات في البيئة بأكملها، لذا ينبغي للمؤسسات التي تشغّل SmartConsole التأكد من تطبيق التحديثات ومراجعة أي مؤشرات إساءة استخدام.

ما يجب فعله الآن

1. التأكد من تطبيق إصلاحات CVE-2026-16232 على Check Point SmartConsole وخوادم الإدارة، وحصر الوصول إلى واجهات الإدارة في شبكات موثوقة.
2. البحث عن مؤشرات الاختراق التي نشرتها GreyNoise في سجلات جدران الحماية وVPN والإدارة، ومنها عناوين IP المذكورة.
3. مراجعة خوادم الإدارة بحثاً عن جلسات مسؤول غير متوقعة وشهادات حديثة الإنشاء وسياسات أمان أُلغي تحميلها وعمليات تصدير للإعدادات.
4. عند الاشتباه بالاختراق، تدوير بيانات الاعتماد ومراجعة جهة إصدار الشهادات الداخلية والشهادات الصادرة عنها.
5. فحص حالة التحديثات للمنتجات المكشوفة الأخرى المذكورة، مثل Citrix NetScaler وIvanti وVMware vCenter وMicrosoft Exchange.
6. إبلاغ الهيئة الوطنية للأمن السيبراني والجهة المنظمة للقطاع عن الحوادث المؤكدة وفق المتطلبات.