

منتجات الشبكة الافتراضية الخاصة من Check Point معرضة لتنفيذ تعليمات برمجية عن بُعد عبر ثغرة في التحقق من الشهادات



تحتوي منتجات Check Point Security Gateway و Spark Firewall التي تستخدم ميزات الشبكة الافتراضية الخاصة على ثغرة في التحقق من الشهادات تتيح للمهاجمين عن بُعد تنفيذ تعليمات برمجية دون مصادقة.

- تؤثر الثغرة على منتجات Check Point Security Gateway و Spark Firewall المهيأة بخاصية Site Remote Access VPN أو Site VPN
- يتيح الخلل في التحقق من الشهادات للمهاجمين عن بُعد دون مصادقة تنفيذ تعليمات برمجية على البوابات المتأثرة
- يجب على المؤسسات تطبيق إجراءات المعالجة من المورد فوراً أو إيقاف استخدام المنتج في حال عدم توفر التحديثات

- تتطلب الأصول المعرضة للإنترنت تقييماً ومعالجة ذات أولوية
- أصدرت CISA توجيهات رسمية تتطلب اتخاذ إجراءات وتطبيق متطلبات الفحص الجنائي

نظرة عامة على الثغرة

تحتوي منتجات Check Point Security Gateway و Check Point Spark Firewall المهية بقدرات Site to Site VPN أو Remote Access VPN على **ثغرة في التحقق من الشهادات** تحمل الرقم التعريفي CVE-2026-85102. يتيح هذا الخلل للمهاجمين عن بُعد دون مصادقة تنفيذ تعليمات برمجية مباشرة على أجهزة البوابات المتأثرة، مما يمثل تعريضاً حرجاً للمؤسسات التي تعتمد على هذه المنتجات لتأمين الاتصال الشبكي.

ينشأ الخلل من عدم كفاية التحقق من الشهادات الرقمية أثناء إنشاء اتصال الشبكة الافتراضية الخاصة، مما يسمح للمهاجمين بتجاوز ضوابط المصادقة دون الحاجة إلى بيانات اعتماد صالحة أو وصول مسبق إلى البيئة المستهدفة.

السياق التنظيمي والتشغيلي

صنفت CISA هذه الثغرة ضمن المعالجات الإلزامية بموجب توجيهاتها BOD 26-04 بشأن تحديد أولويات التحديثات الأمنية بناءً على المخاطر. حددت الوكالة متطلبات الفحص الجنائي للأنظمة المتأثرة ووضعت موعداً نهائياً فيدرالياً للمعالجة في 25 سبتمبر 2026. يُطلب من المؤسسات تطبيق إجراءات المعالجة المقدمة من المورد فوراً أو إيقاف استخدام المنتجات المتأثرة في حال عدم توفر التحديثات.

بالنسبة للمؤسسات الخاضعة للتنظيم في المملكة العربية السعودية، تمثل هذه الثغرة أثراً على الامتثال بموجب الأطر التي تتطلب تصحيح البنية التحتية الحرجة في الوقت المناسب وضوابط الوصول عن بُعد الآمنة. تؤدي قدرة تنفيذ التعليمات البرمجية عن بُعد وعدم الحاجة إلى مصادقة إلى رفع مستوى المخاطر بشكل كبير.

متطلبات الاستجابة الفورية

يجب على المؤسسات جرد جميع عمليات نشر بوابات Check Point، وخاصة تلك التي تحتوي على ميزات الشبكة الافتراضية الخاصة المفعلة والمعرضة للإنترنت. ينبغي لأصحاب المصلحة تقييم ملف التعرض لكل أصل وتحديد أولويات المعالجة وفقاً للأهمية التشغيلية وسطح الهجوم. يجب الرجوع إلى إرشادات المورد للحصول على خطوات المعالجة المحددة، ومراجعة إجراءات الجاهزية الجنائية لضمان الامتثال لالتزامات الاستجابة للحوادث.

ما يجب فعله الآن

1. إجراء جرد فوري لجميع عمليات نشر Check Point Security Gateway و Spark Firewall التي تحتوي على ميزات الشبكة الافتراضية الخاصة المفعلة
2. تحديد بوابات الشبكة الافتراضية الخاصة المواجهة للإنترنت وتقييم ملف تعرضها وأهميتها التشغيلية
3. الرجوع إلى نشرات Check Point الاستشارية للحصول على تعليمات المعالجة المحددة وتطبيق التحديثات أو الحلول البديلة فوراً
4. في حال عدم توفر إجراءات المعالجة من المورد، الاستعداد لإيقاف استخدام المنتجات المتأثرة وتنفيذ حلول بديلة للوصول الآمن عن بُعد
5. مراجعة وتفعيل إجراءات الفحص الجنائي للأنظمة المتأثرة وفقاً لخطط الاستجابة للحوادث

6. توثيق إجراءات المعالجة والجداول الزمنية لإعداد تقارير الامتثال للهيئة الوطنية للأمن السيبراني أو مؤسسة النقد العربي السعودي حسب القطاع المعني