

ثغرة اجتياز المسار في منتجات إدارة Check Point تتيح هجمات غير مصادق عليها



تحتوي منتجات Check Point لإدارة الأمن السيرياني على ثغرة اجتياز مسار تتيح للمهاجمين غير المصادق عليهم رفع وتنفيذ نصوص برمجية تعسفية.

- تأثرت منتجات إدارة متعددة من Check Point بما في ذلك Security Management Serverg Log Serverg Multi-Domain Security Management Serverg SmartEventg
- تتيح الثغرة للمهاجمين غير المصادق عليهم رفع وتنفيذ نصوص برمجية تعسفية عبر اجتياز المسار
- تطالب CISA الجهات الفيدرالية بتطبيق تدابير المورّد الوقائية بحلول 25 سبتمبر 2026
- يجب على المؤسسات تقييم تعرض الأصول المتأثرة للإنترنت وإعطاء الأولوية للترقيع
- يُوصى بوقف استخدام المنتج في حال عدم توفر تدابير وقائية من المورّد

نظرة عامة على الثغرة

أفصحت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA) عن **CVE-2026-93616**، وهي ثغرة اجتياز مسار تؤثر على منتجات إدارة متعددة من Check Point. تؤثر الثغرة على Multi-Domain Security Management Server و Log Server و Security Management Server و Multi-Domain Log Server و SmartEvent. تتيح الثغرة **لمهاجم غير مصادق عليه** رفع وتنفيذ نصوص برمجية تعسفية على الأنظمة المتأثرة، مما يشكل خطراً كبيراً على المؤسسات التي تعتمد على هذه المنصات لإدارة الأمن السيبراني.

المخاطر على المؤسسات السعودية

تمكّن ثغرات اجتياز المسار المهاجمين من الوصول إلى ملفات ومجلدات خارج النطاق المقصود، وفي هذه الحالة، تنفيذ شيفرات خبيثة دون مصادقة. بالنسبة للمؤسسات الخاضعة للتنظيم في المملكة التي تشغل بنية Check Point الإدارية، يمثل هذا تعرضاً حرجاً، خاصة للأنظمة المتاحة عبر الإنترنت. قد تتيح الثغرة للخصوم اختراق منصات إدارة الأمن التي تتحكم في دفاعات الشبكة الأوسع.

إرشادات المعالجة

تشير إرشادات CISA إلى إطار عمل BOD 26-04 الخاص بها لتحديد أولويات التحديثات الأمنية بناءً على المخاطر ومتطلبات الفرز الجنائي. يُطلب من المؤسسات تطبيق التدابير الوقائية التي يوفرها المورد فوراً. وحيث لا تتوفر تدابير وقائية، يُوصى بوقف استخدام المنتج المتأثر. تواجه الجهات الفيدرالية في الولايات المتحدة موعداً نهائياً للمعالجة في 25 سبتمبر 2026، مما يوفر جدولاً زمنياً مرجعياً للإلحاح.

يجب على المؤسسات تقييم أصول إدارة Check Point المعرضة للإنترنت وإعطاء الأولوية للترقية وفقاً لذلك. تتطلب عمليات النشر السحابية اهتماماً خاصاً لضمان اتباع الإرشادات المعمول بها.

ما يجب فعله الآن

1. حدد جميع عمليات نشر Multi-Domain Security و Check Point Security Management Server و Log Server و Management Server و Multi-Domain Log Server و SmartEvent في بيئتك
2. قيّم تعرض كل أصل إداري متأثر من Check Point للإنترنت ووثّق إمكانية الوصول الخارجي
3. اتصل بـ Check Point فوراً للحصول على الترقيات أو التدابير الوقائية التي يوفرها المورد لـ CVE-2026-93616
4. طبّق التدابير الوقائية من المورد على جميع الأنظمة المتأثرة مع إعطاء الأولوية للأصول المواجهة للإنترنت أولاً
5. راجع السجلات للبحث عن مؤشرات الاختراق بما في ذلك رفع ملفات غير متوقعة أو تنفيذ نصوص برمجية على منصات الإدارة
6. إذا لم تتوفر تدابير وقائية من المورد، أعد خطط طوارئ لوقف استخدام المنتجات المتأثرة أو عزلها عن الوصول للإنترنت