CISA تحذر من ثغرة في Check Point Gaia OS تتيح تنفيذ أوامر بصلاحيات الجذر محليًا (CVE-2026-123039)



أدرجت CISA الثغرة CVE-2026-123039 في خدمة DynamicCLI ضمن Gaia OS في عدة منتجات Check Point، وتتيح لمستخدم محلي موثّق تنفيذ أوامر بصلاحيات الجذر. يُنصح بتطبيق إجراءات المورّد.

- الثغرة CVE-2026-123039 تتعلق بمنح صلاحيات غير صحيحة لمورد حرج.
- المنتجات المتأثرة: Multi-Domain Security Management Serverg Check Point Firewall Security Management Serverg Security Gatewayg Scalable Platformsg.
- خدمة DynamicCLI في Gaia OS تعمل بصلاحيات الجذر وتستمع على مقبس محلي قابل للكتابة من الجميع دون التحقق من هوية المتصل.
- يستطيع مستخدم محلي موثّق إرسال أمر إلى المقبس لينفَّذ بصلاحيات الجذر.
- تطلب CISA تطبيق إجراءات المورّد، والموعد النهائي للجهات الفيدرالية الأمريكية 2026-11-16.

أضافت CISA الثغرة CVE-2026-123039 إلى قائمة الثغرات التي تستوجب إجراءً. وتمس عدة منتجات من Check Point هي: Firewall وSecurity Gateway وScalable Platforms وMulti-Domain Security Management Server وSecurity Management Server.

طبيعة الثغرة

تعمل خدمة DynamicCLI في Gaia OS بصلاحيات الجذر وتستمع على مقبس محلي يمكن لأي حساب محلي الكتابة إليه، ولا تتحقق من هوية العمليات المتصلة بها. ونتيجة لذلك يستطيع مستخدم محلي موثّق إرسال أمر إلى المقبس فيُنفَّذ بصلاحيات الجذر.

يصف المصدر مسار هجوم محليًا يتطلب حسابًا على الجهاز، لكن نتيجته سيطرة إدارية كاملة على جهاز أمني، ما يجعل المسألة مهمة لكل جهة تعتمد على هذه المنتجات عند حدود الشبكة أو في الإدارة المركزية.

ما تطلبه CISA

توجّه CISA الجهات إلى تطبيق إجراءات التخفيف وفق تعليمات المورّد، بما يتوافق مع إرشادات BOD 26-04 لترتيب أولوية التحديثات الأمنية بحسب المخاطر ومتطلبات الفرز الجنائي الرقمي. وإذا لم تتوفر إجراءات تخفيف فيُتّبع ما ينطبق من إرشادات BOD 26-04 للخدمات السحابية أو يُتوقف عن استخدام المنتج. وتتحمل كل جهة مسؤولية تقييم تعرّض أصولها للإنترنت. والموعد النهائي للجهات الفيدرالية الأمريكية هو 2026-11-16.

قراءة عملية

لا تلتزم الجهات السعودية بـ BOD 26-04، لكنه مرجع مفيد. والأولوية هي حصر أنظمة Check Point المتأثرة، وتطبيق إجراءات المورّد، ومراجعة من يملك وصولاً محليًا إليها.

ما يجب فعله الآن

1. حصر جميع أنظمة Check Point من نوع Firewall وSecurity Gateway وSecurity Management Server وMulti-Domain وScalable Platforms التي تعمل على Gaia OS.
2. تطبيق إجراءات التخفيف الواردة في تعليمات المورّد، بدءًا بالأنظمة المكشوفة للإنترنت وأنظمة الإدارة.
3. مراجعة حسابات الوصول المحلي وصدفة الأوامر على هذه الأجهزة وحصرها في الحد الضروري.
4. فحص السجلات ونشاط الحسابات على الأجهزة المتأثرة بحثًا عن أوامر محلية غير متوقعة أو تغييرات في الصلاحيات، مع حفظ الأدلة عند وجود أي مؤشر.
5. توثيق القرار والجدول الزمني ضمن إدارة الثغرات بما يتوافق مع متطلبات ضوابط NCA ECC وإطار SAMA CSF.