هذه الوثيقة هي ترجمة للنسخة الإنجليزية التالية https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/. ونقدّم هذه النسخة المترجمة لسهولة المرجع ولأغراض تعريفية فقط. وفي حال وجود أي تعارض أو غموض، يحتكم إلى النسخة الإنجليزية دائمًا، وتكون لها الأولوية

ملخص تنفيذي

المراجعة الأولية لما بعد الحادث (PIR) التي أجرتها CrowdStrike: تحديث تهيئة المحتوى الذي يؤثر في مستشعر Falcon ونظام التشغيل Windows (عطل الشاشة الزرقاء)

نظرة عامة

لمواجهة التهديدات السيبرانية الجديدة والمتنامية، تصدر منتجات الأمن السيبراني تحديثات دورية للمحتوى. يمكن أن تتضمن هذه التحديثات جمع البيانات عن بُعد، وأنماطًا جديدة للكشف عن التهديدات، واكتشاف الثغرات الأمنية، وغير ذلك من التحسينات بالغة الأهمية. ومن خلال هذه التحديثات الدورية، يمكن لمنتجات الأمن السيبراني التكيف سريعًا لمواجهة التهديدات الناشئة، ما يضمن توفير حماية قوية للمستخدمين وأنظمتهم.

ماذا حدث: نظرة عامة على الحادث

في 19 يوليو 2024، الساعة 04:09 بالتوقيت العالمي الموحد، تم نشر تحديث محتوى الاستجابة السريعة لمستشعر Falcon على الأجهزة التي تعمل بنظام التشغيل Windows التي تستخدم إصدار المستشعر 7.11 والإصدارات الأحدث. كان الهدف من هذا التحديث جمع البيانات عن بُعد حول تقنيات التهديد الجديدة التي رصدتها CrowdStrike، لكنه تسبب في حدوث أعطال (عطل الشاشة الزرقاء) على الأنظمة التي كانت متصلة بالإنترنت بين الساعة 04:09 والساعة 05:27 بالتوقيت العالمي الموحد. ولم تتأثر الأجهزة التي تعمل بنظام التشغيل Mac ونظام التشغيل Linux بهذا الحدث. وكذلك لم تتأثر الأجهزة التي تعمل بنظام التشغيل Windows التي لم تكن متصلة بالإنترنت أو التي لم تنشئ اتصالاً خلال هذه الفترة.

لماذا حدث ذلك: سبب الحادث

حدثت الأعطال بسبب خلل في محتوى الاستجابة السريعة لم يتم اكتشافه أثناء عمليات التحقق من صحة البيانات. وعندما تم تحميل المحتوى بواسطة مستشعر Falcon، تسبب هذا في قراءة ذاكرة خارج الحدود، ما أدى إلى تعطل أنظمة التشغيل Windows (عطل الشاشة الزرقاء).

ما الإجراءات التي تتخذها CrowdStrike لتفادي حدوث ذلك مرة أخرى؟

تحسين إجراءات اختبار البرامج

- تحسين اختبار محتوى الاستجابة السريعة من خلال استخدام أنواع اختبارات مثل: اختبار المطور المحلي، واختبار تحديث المحتوى والتراجع عنه، واختبار الإجهاد، واختبار القيم المحتملة، واختبار إدخال الأخطاء، واختبار الاستقرار، واختبار واجهة المحتوى.
- استحداث عمليات تحقق إضافية للتحقق من الصحة في مدقق المحتوى لتفادي حدوث مشكلات مماثلة.

تعزيز المرونة والقدرة على التعافي

- تعزيز آليات معالجة الأخطاء في مستشعر Falcon؛ لضمان التحكم في الأخطاء الناتجة عن المحتوى المسبب للمشكلة وإدارتها بسلاسة.

تحسين إستراتيجية النشر

- تبني إستراتيجية نشر مُتدرجة، بدءًا من عمليات النشر المرحلي إلى مجموعة فرعية صغيرة من الأنظمة قبل النشر على نطاق أوسع.
- تعزيز مراقبة أداء المستشعر والنظام أثناء النشر المتدرج للمحتوى؛ لتحديد المشكلات والتخفيف من آثارها على الفور.
- منح العملاء قدرة أوسع على التحكم في تلقي تحديثات محتوى الاستجابة السريعة، من خلال السماح بالتحديد الدقيق لوقت نشر هذه التحديثات ومكان نشرها.
- تقديم إشعارات بتحديثات المحتوى وتوقيتها.

التحقق من موارد الجهات الخارجية ومراجعتها

- إجراء مراجعات مستقلة متعددة للأكواد البرمجية الخاصة بالأمان التي تقدمها جهات خارجية.
- إجراء مراجعات مستقلة لعمليات الجودة الشاملة؛ بداية من التطوير وحتى النشر.