ماذا يحتوي برنامجك؟ قوائم (SBOM) وأمن سلسلة التوريد

أليكسيوس زافراس



الملخص:

يعرف المقال قائمة مكونات البرمجيات (SBOM) بوصفها سجلًا يصف مكونات المنتج وإصداراتها ومصادرها وعلاقاتها، ودورها في فهم سلسلة التوريد. ويشرح انتقال الاهتمام بها من حصر التزامات التراخيص إلى دعم الأمن والتعامل مع الثغرات، مع إبراز أهمية صيغة متفق عليها لتبادل البيانات. ويعرض معيار (SPDX) ونشأته التعاونية، وتمييزه بين تسجيل الوقائع والتفسير القانوني، وإمكان تمثيله بصيغ متعددة. كما يوضح مستويات الوثيقة من الحزم إلى الملفات ومقاطع الشيفرة، وتفاوت درجة التفصيل بحسب الحاجة، وأنواع الأدوات التي تنتج القوائم أو تحللها. ويناقش التطوير الوحداتي المرتقب وقت الأصل، ويؤكد أن البيانات المنظمة تسهل التواصل والامتثال وإدارة المخاطر عبر مراحل بناء البرمجيات وتبادلها وصيانتها، بما يخدم مختلف الجهات المشاركة في سلسلة التوريد.

الكلمات المفتاحية: قائمة مكونات البرمجيات، (SBOM)، (SPDX)، أمن سلسلة التوريد، تراخيص البرمجيات

حتى سنوات قليلة مضت، كانت قاعدة 80/20 صالحة: ينبغي ألا يكون 80% من محتوى أي برنامج مهم من تطويرك أنت. فلا معنى اقتصاديًا لتطوير أكثر من 20%، لأن آخرين بنوا غالبًا مكونات تؤدي الوظائف المطلوبة. والأفضل التركيز على ما يمنحك ميزة تنافسية. وربما تحولت النسبة في السنوات الأخيرة إلى 90/10.

هنا تأتي قائمة مكونات البرمجيات (SBOM): سجل رسمي يضم تفاصيل المكونات المستخدمة في بناء البرنامج وعلاقات سلسلة توريدها. وقد تكون مفتوحة أو مملوكة، مجانية أو مدفوعة، متاحة للجميع أو مقيدة الوصول. وتساعد معلوماتها في الإجابة عن أسئلة تعاقدية وقانونية وتقنية متنوعة.

كان الامتثال القانوني دافعًا رئيسيًا للمحاولات المبكرة. فكل مكون يخضع لترخيص قد يفرض التزامات، ويتطلب الامتثال الوفاء بالتزامات التراخيص كلها؛ وهو واضح من حيث المبدأ، لكنه صعب التنفيذ. والخطوة الأولى البديهية سجل لجميع المكونات وتراخيصها، وهذا ما تقدمه (SBOM).

لكن هجمات سلسلة التوريد في السنوات السابقة جعلت الأمن الدافع الأساسي لمعرفة ما داخل البرنامج بدقة، وأصبح متوقعًا إرفاق القائمة ببعض أشكال التسليم. ويشير الكاتب مثالًا إلى الأمر التنفيذي الأمريكي 14028 الذي يدعو الجهات الحكومية إلى بدء طلب هذه القوائم للمنتجات البرمجية والعتادية التي تقتنيها.

قائمة مكونات البرمجيات:

تشبه على المستوى المفاهيمي فهرس محتويات بسيطًا: قائمة شاملة بالمكونات وأسمائها وإصداراتها ومصادرها، وربما معلومات التراخيص والثغرات وسلسلة المنشأ أو أي جانب آخر. ويمكن تمثيلها في جدول أو وثيقة نصية أو ملف جداول. ولكي تفيد، يجب أن يفهم طرفا التبادل الصيغة ويتفقا عليها.

تبادل بيانات الحزم البرمجية (SPDX):

قبل أكثر من عشر سنوات، بدأ ممثلون عن شركات مختلفة العمل على تحديد صيغة مشتركة موحدة أسموها (SPDX). واتفقوا على ألا تمنح شركة بعينها ميزة تنافسية، فجرى العمل وفق مبادئ المصدر المفتوح كاملة وبمشاركة مفتوحة للجميع.

(SPDX) معيار مفتوح لنقل معلومات (SBOM)، ويشير الأصل إلى اعتماده معيارًا دوليًا باسم (ISO/IEC 5962:2021). وتُنتج مواصفته تعاونيًا بمشاركة مجموعات عمل بحسب الاهتمام والخبرة. وكانت (Intel) مشاركة منذ البداية في فرق منها التقني للمواصفة، والقانوني لقائمة التراخيص، والتوعوي لترويج الاستخدام.

يقوم (SPDX) على تسجيل الوقائع. فهو يسجل مثلًا الترخيص المعلن للمكون، ويتجنب تفسير شروطه أو التزاماته قانونيًا. كما يدعم ترميز المعلومات بصيغ متعددة، منها النص محدود البنية و (JSON) و (XML) و (RDF) وحتى الجداول.

وبنية الوثيقة هرمية؛ فإلى جانب معلوماتها العامة كالمؤلف والتاريخ، تُعرض المعلومات بمستويات متزايدة من التفصيل: الحزم والملفات ومقاطع الشيفرة. ومعظم المعلومات في كل مستوى اختياري، فيمكن إنشاء قائمة عامة أو بالغة التفصيل، مما يجعل الصيغة مناسبة لحالات واقعية متعددة. فقد يهتم أحد متلقي القائمة بالثغرات وحدها، ويهتم آخر بالتراخيص والتزاماتها.

وتتعامل أدوات كثيرة مع وثائق (SPDX)، ويمكن تصنيفها وفق الوظيفة والمرحلة من سلسلة التوريد. فقد تُنتج الوثيقة أثناء البناء، أو بعده بتحليل البرنامج المبني. وتستخدم أدوات أخرى هذه المعلومات لتحليل الوثائق أو تحويلها أو مقارنتها أو دمجها.

وتعمل المجموعات، وقت كتابة الأصل، على الإصدار الرئيسي التالي (SPDX 3)، لإعادة تنظيم المعلومات في وحدات وأقسام منفصلة. فيمكن مثلًا إبراز الأمن والثغرات وتقليل تفاصيل التراخيص. ومع اتساع الاستخدامات، يتوقع الكاتب أن يدعم هذا النهج مزيدًا من التبني.

ويشير المقال إلى مشاركة الكاتب بحديث عن (SBOM) و (SPDX) في مؤتمر البرمجيات الحرة بجنوب تيرول (SFSCON) لسنة 2023.

المراجع:

- https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
- https://spdx.dev/about
- https://www.iso.org/standard/81870.html
- https://github.com/spdx/spdx-3-model
- https://www.sfscon.it/talks/software-bills-of-materials-sbom
- https://www.sfscon.it
- https://pixabay.com/users/riedelmeier-130476/?utm_source=link-attribution&utm_medium=referral&utm_campaign=image&utm_content=616573
- https://pixabay.com//?utm_source=link-attribution&utm_medium=referral&utm_campaign=image&utm_content=616573
- https://opensource.net/author/zvr/