
EUA e 14 aliados divulgam orientação conjunta sobre lista de materiais de

Data: 2025-09-04 17:47:24

Autor: Inteligência Against Invaders

Em uma colaboração histórica, agências de segurança cibernética e inteligência de 15 países se alinharam em uma visão compartilhada para [Listas de materiais de software](#) (SBOMs), emitindo novas orientações conjuntas para fortalecer a segurança da cadeia de suprimentos global.

O documento, intitulado “[Uma visão compartilhada da lista de materiais de software \(SBOM\) para segurança cibernética](#)“, foi publicado em 3 de setembro.

Foi assinado por 21 agências governamentais de 15 países, incluindo a Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA) e a NSA.

Ele descreve os principais termos e conceitos relacionados aos SBOMs, incluindo uma definição comum do que é um SBOM, a proposta de valor dos SBOMs e como implementá-los.

Ele descreve as funções dos produtores de SBOM, usuários finais (chamados de “selecionadores” no documento), operadores e organizações nacionais de segurança cibernética.

Além disso, a orientação incentiva a adoção generalizada de SBOM em todos os setores e fronteiras, implementações técnicas harmonizadas para reduzir a complexidade e o custo e integração de SBOMs em fluxos de trabalho de segurança para melhor gerenciamento de riscos.

“Este marco reflete um crescente consenso internacional sobre a importância da transparência do software na proteção da cadeia de suprimentos digital”, comentou um porta-voz da CISA.

Lukáš KINTR, diretor da Agência Nacional de Segurança Cibernética e da Informação da República Tcheca (NÚKIB), um dos signatários, enfatizou a crescente complexidade do software que as organizações devem enfrentar.

“O software de hoje geralmente consiste em centenas de componentes originários de várias fontes e bibliotecas. O SBOM traz transparência essencial a esse ambiente complexo e mostra claramente do que o software é feito. Considero o SBOM um passo fundamental para a criação de software verdadeiramente seguro e resiliente – já desde o seu design”, disse ele.

Nobutaka Takeo, diretor da Divisão de Segurança Cibernética do Departamento de Política de Comércio e Informação do Ministério da Economia, Comércio e Indústria do Japão (METI), declarou: “Estamos satisfeitos em ver que a importância do SBOM está sendo reconhecida internacionalmente por meio desta diretriz. No ano passado, o Japão lançou o SBOM Guidance 2.0 e continuaremos a aumentar a conscientização sobre o SBOM entre as partes interessadas relevantes, contribuindo ativamente para as discussões internacionais sobre o assunto.”

Trabalhando para a harmonização e legislação da SBOM

Allan Friedman, que liderou os esforços de SBOM da CISA entre agosto de 2021 e julho de 2025, saudou a publicação da orientação conjunta.

Em um post no LinkedIn, ele enfatizou que era “o maior número de organizações que já aderiram à CISA em um documento internacional”.

“Não há nada aqui inovador, mas é ótimo ter uma contribuição tão ampla de tantos países”, acrescentou, antes de sugerir que ainda são necessários mais passos, incluindo a harmonização das implementações técnicas.

“Implementações divergentes podem impedir a adoção generalizada e a implementação sustentável do SBOM. Uma abordagem alinhada e coordenada para o SBOM melhorará a eficácia e reduzirá custos e complexidades”, disse ele.

Falando com *Segurança da informação*, Josh Bressers, vice-presidente de segurança da Anchore e líder do grupo de trabalho OpenSSF SBOM Everywhere, descreveu o esforço como uma iniciativa “ótima”.

No entanto, ele corroborou a visão de Friedman, afirmando que este acordo de alto nível é apenas “o primeiro passo lógico para ver uma adoção global da transparência do software por meio de SBOMs”.

O desejo de Bressers para o próximo passo é ver legislação e orientação comuns sobre a segurança da cadeia de suprimentos de software entre os países signatários.

“A maioria dos produtores opera em um cenário global agora, [regulations] como a da UE [Lei de Resiliência Cibernética \(CRA\)](#) vão afetar um grande número de empresas. Sem dúvida, outros países criarão orientações semelhantes. Se não tivermos uma visão comum, será muito difícil atender a todos os requisitos”, concluiu.

Além da CISA, da NSA, do NÚKIB e do METI, as organizações signatárias incluíram:

-
- Centro Australiano de Segurança Cibernética da Diretoria de Sinais Australiano (ASD's ACSC)
 - O Centro Canadense de Segurança Cibernética (Cyber Centre)
 - A Agência Francesa de Segurança Cibernética (ANSSI)
 - Escritório Federal de Segurança da Informação da Alemanha (BSI)
 - A Equipe Indiana de Resposta a Emergências de Computadores (CERT-In)
 - Nat da Itália Agência Nacional de Cibersegurança (ACN)
 - Escritório Nacional de Segurança Cibernética do Japão (NCO)
 - Centro Nacional de Segurança Cibernética da Holanda (NCSC-NL)
 - Centro Nacional de Segurança Cibernética da Nova Zelândia (NCSC-NZ)
 - Rede de Computadores Acadêmicos e de Pesquisa da Polônia (NASK)
 - A Agência de Segurança Cibernética de Cingapura (CSA)
 - Autoridade Nacional de Segurança da Eslováquia (NBÚ)
 - Serviço Nacional de Inteligência da Coreia do Sul/Centro Nacional de Segurança Cibernética (NIS/NCSC) e Agência Coreana de Internet e Segurança (KISA)

[Leia mais: CISA busca mudança na diretriz de requisitos mínimos de SBOM da era Biden](#)