

O Docker torna o Catálogo de Imagens Reforçadas acessível para pequenas empresas

Data: 2025-10-07 22:23:08

Autor: Inteligência Against Invaders

A equipe do Docker anunciou acesso ilimitado ao seu catálogo Hardened Images para tornar o acesso a pacotes de software seguros acessível para todas as equipes de desenvolvimento em startups e PMEs.

A partir de hoje, as imagens de contêiner que foram verificadas como livres de vulnerabilidades conhecidas (CVEs quase zero) estão disponíveis para todos os usuários por meio de uma assinatura e uma avaliação gratuita de 30 dias.

“Estamos introduzindo acesso ilimitado ao catálogo Docker Hardened Images, tornando os CVEs quase zero uma realidade prática para todas as equipes a um preço acessível” [Leia o anúncio](#).

“Com uma única assinatura do Hardened Images, todas as equipes podem acessar o catálogo completo: ilimitado, seguro e sempre atualizado.”

O Docker é uma plataforma amplamente utilizada que permite aos desenvolvedores empacotar aplicativos e suas dependências em “contêineres”, permitindo uma implantação consistente e sistemática em diferentes ambientes.

As imagens de contêiner são modelos que incluem todo o código, tempo de execução, bibliotecas e ferramentas do sistema necessários para executar um aplicativo.

Risco de segurança reduzido

Imagens reforçadas são [Versões altamente seguras](#) de imagens regulares do Docker que eliminam o risco de vulnerabilidades conhecidas, pois são criadas a partir do código-fonte, se beneficiam de patches upstream contínuos e carecem de componentes desnecessários.

Cada imagem reforçada também inclui suporte para Vulnerability Exploitability eXchange (VEX), que coloca os holofotes apenas em questões de segurança que realmente importam.

Além disso, o Docker diz que, removendo conteúdo não essencial, a superfície de ataque diminui em até 95%.

O Docker fez parceria com auditores independentes de segurança cibernética da SRLabs, que validaram que as imagens protegidas são assinadas adequadamente, sem raiz por padrão, incluem SBOM e VEX e não mostraram escapes de raiz ou outros problemas de breakout de alta gravidade.

As imagens protegidas também são sustentadas por um SLA (Contrato de Nível de Serviço) de

patch de sete dias, o que significa que, quando um novo CVE afeta um componente usado na imagem, o Docker deve lançar uma versão corrigida dentro de uma semana.

O catálogo Hardened Images oferece uma ampla variedade de imagens, inclusive para inteligência artificial/aprendizado de máquina, linguagens e tempos de execução (Python), bancos de dados (PostgreSQL), estruturas (NGINX) e ferramentas de infraestrutura (Kafka).

O catálogo também apresenta variantes prontas para FedRAMP que atendem aos padrões de segurança federais mais rígidos dos EUA.

Todas as imagens do catálogo Hardened Images são compatíveis com os sistemas Alpine e Debian Linux, podem ser facilmente integradas alterando uma única linha do Dockerfile e podem ser personalizadas livremente sem perder a linha de base reforçada.

O Docker Hub continua sendo o ponto de partida padrão para a maioria das compilações de contêiner, mas a liberação do catálogo de Imagens Reforçadas para todos os usuários pode marcar o início de uma elevação significativa na segurança do ecossistema.

[\[IMAGEM REMOVIDA\]](#)

-

O Evento de Validação de Segurança do Ano: O Picus BAS Summit

Junte-se ao **Cúpula de Simulação de Violção e Ataque** e experimente o **Futuro da validação de segurança**. Ouça os principais especialistas e veja como **BAS alimentado por IA** está transformando a simulação de violação e ataque.

Não perca o evento que moldará o futuro da sua estratégia de segurança