# APPLICATION SECURITY 101

A crescente complexidade das aplicações, sua dependência de bibliotecas de terceiros e a velocidade e escala oferecidas pelo DevOps e pela nuvem os tornam vulneráveis a ataques.

A maioria dos ataques externos relatados em 2019 foram realizados por meio de


Exploração de uma falha de software

Comprometimento de uma aplicação da web

Na última década,[2] as violações causadas por ataques de aplicações foram responsáveis por


do custo do comprometimento

do total de registros expostos

**9** das **10** principais imagens de contêiner oficiais no Docker Hub continham mais de 50 vulnerabilidades.[3]

## PRINCIPAIS RISCOS PARA APLICAÇÕES DA WEB

### COMPONENTES VULNERÁVEIS

Componentes com vulnerabilidades conhecidas permitem que os invasores conduzam vários ataques.

### EXPOSIÇÃO DE DADOS SENSÍVEIS

Aplicações da Web e APIs podem falhar na proteção adequada de dados confidenciais.

### FRACO CONTROLE DE ACESSO DE BACKEND

Controles de acesso de backend fracos permitem que os agentes da ameaça ignorem a autorização e executem tarefas.

### INJEÇÃO

As falhas de injeção podem ser exploradas para iniciar quando dados não confiáveis são enviados a um intérprete de código e, em seguida, executados.

### CONFIGURAÇÃO INCORRETA DE SEGURANÇA

Erros em configurações podem acontecer por causa do uso de padrões inseguros nelas.

### AUTENTICAÇÃO QUEBRADA

O comprometimento pode surgir quando as funções da aplicação, como autenticação e gerenciamento de sessão, estão incorretas.

### SCRIPTS ENTRE SITES (XSS)

As falhas de XSS ocorrem se uma aplicação incluir dados não testados em uma nova página da Web sem validação ou escape adequados.

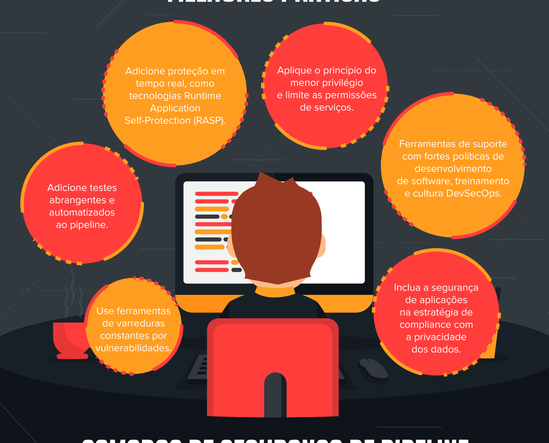
### DESSERIALIZAÇÃO INSEGURA

Falha na desserialização pode permitir que os agentes de ameaças executem ataques de reprodução, injeção e escalonamento de privilégios.

### REGISTRO E MONITORAMENTO INSUFICIENTES

Mecanismos insuficientes para detectar comprometimento podem permitir que os agentes de ameaças ataquem ainda mais os sistemas e adulterem, extraiam ou destruam dados.

## MELHORES PRÁTICAS




## CAMADAS DE SEGURANÇA DE PIPELINE

Análise de composição de software

Teste de segurança de aplicações estáticas, dinâmicas e interativas

Verificação e segurança de contêineres

Varredura de Dependências

## SOLUÇÕES TREND MICRO

Trend Micro Cloud One™ – Application Security protege automaticamente as aplicações contra ataques comuns baseados na web e muitas classes de vulnerabilidades de zero-day.

O Application Security faz parte da plataforma de serviços de segurança Trend Micro Cloud One, que também inclui outros serviços de segurança para o desenvolvimento de aplicações nativas da nuvem, como Container Security, File Storage Security e Workload Security, junto com Network Security e Conformity.

---

1 Sandy Carielli, Forrester, "The State Of Application Security 2020."
2 Sara Boddy e Raymond Pompon, F5 Labs, "Lessons Learned From a Decade of Data Breaches."
3 Snyk, "State of Open Source Security Report 2020."



TREND MICRO | research