Número 110 | Janeiro 2026

NTT DATA

Radar

A revista de cibersegurança

A cibersegurança como um habilitador de negócios

Por Maria Pilar Torres Bruna

Bem-vindo, 2026! Iniciamos um novo ciclo marcado por um cenário tecnológico tão empolgante quanto desafiador. Os negócios estão cada vez mais atrelados à tecnologia que os sustenta, e a rápida evolução da inteligência artificial — que deixou de ser apenas preditiva, passou pela fase generativa e agora entra em uma **era agêntica** — está impulsionando a criação de agentes digitais capazes de aprimorar o potencial do trabalho humano.

A computação quântica, tema cada vez mais presente nas discussões do setor, deixará de ser um conceito distante para se tornar realidade nos próximos anos. Diversas organizações já começam a explorar novos modelos de negócio e ganhos de eficiência baseados nessa tecnologia, ao mesmo tempo que se preparam para as **novas ciberameaças** que ela inevitavelmente trará.

Nós, profissionais de cibersegurança, compartilhamos o entusiasmo do setor diante dessas transformações. Mas também sabemos que a cibersegurança já não é apenas um acelerador dos negócios — hoje é um dos **principais habilitadores**. Sem cibersegurança, simplesmente não há continuidade, inovação ou confiança.

Neste início de ano, quero destacar os **três pilares fundamentais** que devem orientar o trabalho de todo CISO. Eles respondem diretamente aos principais desafios enfrentados pelas organizações em matéria de segurança e formam a base da nossa atuação na NTT DATA como companhia global. É a partir desses pilares que estruturamos os serviços que levaremos ao mercado nos próximos anos:

1. Gestão de riscos e conformidade proativa

Toda iniciativa de cibersegurança deve nascer de um risco bem definido — e contribuir para sua mitigação. Além disso, é fundamental adotar uma abordagem contínua de revisão e adaptação, antecipando-se aos riscos emergentes gerados por técnicas de ataque cada vez mais sofisticadas.

2. Impulsionar um negócio seguro

O CISO deve ocupar um papel estratégico no *C-level*, garantindo que os objetivos de cibersegurança estejam completamente integrados às metas corporativas. Também é sua responsabilidade construir **casos de valor** que fortaleçam a confiança de clientes, colaboradores e *stakeholders* na organização.

3. Ciberresiliência

A resiliência tornou-se um conceito indispensável. Toda disrupção representa perdas, mas o verdadeiro diferencial competitivo está na capacidade de resposta: a **agilidade com que uma organização se recupera** de um incidente e minimiza seus impactos operacionais e financeiros.

Em 2026, continuaremos comprometidos em ajudar as organizações a se fortalecerem em torno desses três pilares. Estou convencida de que nós, profissionais da área de cibersegurança, temos um papel fundamental na evolução das empresas nos próximos anos — e é justamente isso que torna nosso trabalho tão fascinante.

A equipe da NTT DATA deseja a todos um 2026 próspero e ciberseguro!

Maria Pilar Torres Bruna
Head of Cybersecurity IBIOL

Shai-Hulud 2.0: o dia em que o malware conheceu toda a cadeia

Cibercrônica por Marlon Nivia Devia

Entre setembro e novembro de 2025, a indústria de *software* descobriu que os ataques à cadeia de suprimentos estavam longe de atingir seu auge — eles estavam apenas começando. O que antes era visto como um risco limitado ao uso de componentes de terceiros evoluiu para uma ameaça estrutural, capaz de comprometer não apenas o código-fonte, mas também os profissionais que o escrevem, empacotam, automatizam e implantam.

A chegada do malware Shai-Hulud, seguida alguns meses depois por sua versão mais avançada, Shai-Hulud 2.0, representou um divisor de águas para o ecossistema tecnológico e para as plataformas de desenvolvimento em cloud. A indústria percebeu que o problema ia muito além do gerenciador de pacotes npm: estava na confiança delegada a um conjunto de automações que ninguém questionava.

A primeira onda veio em setembro de 2025, quando pesquisadores revelaram um ataque de package poisoning no npm com capacidade de propagação autônoma. Foi classificado como uma infecção massiva: dezenas de pacotes modificados, milhares de downloads comprometidos e um efeito dominó que se espalhava rapidamente — mas que, a princípio, parecia restrito ao repositório. Essa leitura se revelou, mais tarde, um falso alívio. Em novembro, surgiu o Shai-Hulud 2.0: um malware mais furtivo, mais consciente do ambiente e com ambições iam além da distribuição de código. O alvo agora não eram apenas as versões publicadas, mas as identidades digitais vinculadas a GitHub, AWS, Google Cloud Platform e Azure. A superfície de ataque se expandiu do package.json à infraestrutura completa onde o *software* é desenvolvido, integrado e executado.

A mudança de foco ficou evidente em suas novas habilidades. Shai-Hulud 2.0 roubava *tokens* do npm, credenciais do GitHub e chaves de API, mas também utilizava esses segredos para invadir os sistemas nativos de gerenciamento de credenciais dos principais provedores de *cloud*: AWS Secrets Manager, Google Secret Manager e Azure Key Vault. Em muitos casos, explorava ainda sistemas legados como o Azure Pod Identity, presente em diversos *clusters* Kubernetes.

O vírus não se limitou a obter informações estáticas, mas compreendeu os aspectos dinâmicos do ambiente: a permissão exata, a variável de *pipeline*, a chave que acessava o ambiente de produção a partir de um sistema que nunca deveria tê-la.

E se o roubo falhasse, o *malware* recorria à sua cartada final: um comportamento destrutivo capaz de apagar diretórios inteiros — como se soubesse que, em uma cadeia de suprimentos rompida, destruir poderia ser tão vantajoso quanto roubar.

O impacto real não foi medido em pacotes infectados, mas sim em segredos expostos. Segundo investigações posteriores, cerca de 400 mil credenciais foram coletadas e disseminadas por meio de dezenas de milhares de repositórios públicos, ficando abertamente disponíveis para qualquer agente que as encontrasse, analisasse ou reutilizasse. O mais alarmante? Muitos desses *tokens* ainda estavam ativos quando a campanha veio à tona.

Enquanto o setor tentava mensurar quantas versões haviam sido comprometidas, uma questão mais urgente se impôs: quem tem acesso a esses dados agora — e há quanto tempo? O que começou como um incidente técnico envolvendo o npm acabou impactando plataformas de integração contínua como GitHub Actions, Jenkins, GitLab CI e AWS CodeBuild, atingindo *pipelines* baseados em containers Linux que automatizavam os processos de publicação e implantação. O ataque provou que não era preciso entrar no modo de produção, uma vez que toda a fábrica que produzia o *software* podia ser controlada.

Para a comunidade de desenvolvimento, o Shai-Hulud 2.0 foi mais do que um malware. Foi um alerta de que o modelo de confiança do *software* moderno precisa ser reavaliado. O código aberto nasce da colaboração. Mas a automação extrema se apoia numa crença cega: de que tudo é seguro — o pacote, o *token*, o *script*. E de que ninguém teria motivos para inserir algo malicioso durante a instalação. Pois, o vírus desmontou essa suposição. Em um mundo onde instalar é o mesmo que executar, cada linha de código baixada representa, na prática, uma decisão de segurança.

Um ano, duas variantes — e uma mensagem clara: a ameaça já não entra pela aplicação, mas por quem a desenvolve.

O Shai-Hulud não apenas roubou segredos, mas expôs uma verdade incômoda: a cadeia de desenvolvimento de *software* é tão robusta quanto sua dependência mais frágil — e tão segura quanto o *token* mais esquecido em uma variável de ambiente. Proteger essa cadeia exige enxergar além do repositório e reconhecer que toda automação, por mais útil que pareça, pode se transformar em uma execução não supervisionada a serviço do invasor.

Marlon Nivia Devia
Cybersecurity Engineer

OWASP TOP 10:2025
Programadores melhores ou *frameworks* mais seguros?

Artigo por Martín Bedoya Rodriguez

Nos últimos anos, os *frameworks* modernos para desenvolvimento de aplicações web, mobile e APIs evoluíram significativamente — não apenas em desempenho e usabilidade, mas também em segurança. Tecnologias como Spring Boot, .NET, FastAPI, React e Flutter passaram a incorporar mecanismos de proteção que ajudam a mitigar vulnerabilidades comuns. Ainda assim, persiste uma lacuna entre o que essas ferramentas oferecem e o nível de consciência das equipes de desenvolvimento sobre práticas seguras de programação.

A mudança também se reflete na forma como o *software* é estruturado. Em vez de aplicações monolíticas, os times vêm adotando arquiteturas modulares que favorecem a separação de responsabilidades. Isso facilita a aplicação de boas práticas de segurança desde as fases iniciais do projeto. No entanto, usar uma arquitetura moderna não garante, por si só, um *software* seguro. A segurança ainda depende, em grande medida, do conhecimento e da capacidade crítica de quem projeta e implementa as soluções.

O OWASP TOP 10 ajuda a entender como as ameaças evoluíram no desenvolvimento de *software*. Trata-se de uma lista hierarquizada que reúne as categorias de vulnerabilidades mais exploradas nos últimos quatro anos — funcionando como um guia prático para que as equipes priorizem ações de segurança ao longo do ciclo de vida do *software*. A versão mais recente, o OWASP TOP 10:2025, traz atualizações importantes que refletem o avanço dos ataques cibernéticos e seus impactos sobre as organizações.

Um dos destaques é a queda da categoria de injeção de código para o quinto lugar. Em 2017, essa vulnerabilidade liderava o ranking; em 2021, havia caído para o terceiro lugar. Agora, segue perdendo relevância. Esse movimento mostra que os controles nativos dos *frameworks* têm surtido efeito. Hoje, a maioria dos *frameworks* já inclui filtros de sanitização, que evitam esse tipo de vulnerabilidade sem exigir ação direta do programador. Mesmo assim, aplicações legadas ou o uso inadequado dos recursos do *framework* ainda representam um risco.

Por outro lado, o primeiro lugar segue ocupado por falhas no controle de acesso — vulnerabilidades que permitem a usuários acessar dados ou funcionalidades que não deveriam estar disponíveis.

Esse tipo de erro é mais difícil de mitigar automaticamente, pois está ligado a como os papéis e permissões são definidos na lógica do *software*. Exige decisões conscientes dos desenvolvedores, que precisam compreender o funcionamento do negócio para criar mecanismos de controle realmente eficazes.

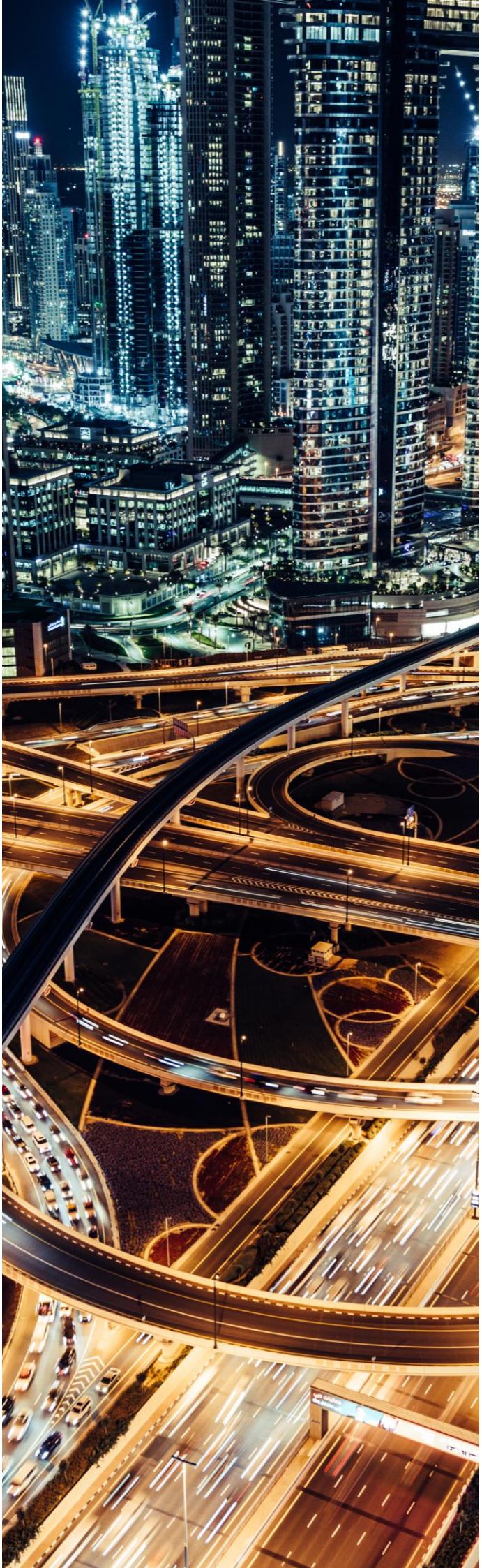
Outra novidade relevante da edição 2025 é a inclusão da categoria “falhas na cadeia de suprimentos de *software*”, que reconhece o risco de depender de bibliotecas externas sem validação adequada. Hoje é comum que uma aplicação utilize dezenas de componentes de terceiros, e basta que um deles apresente uma vulnerabilidade para comprometer toda o *software*. A categoria cita inclusive técnicas emergentes como o *typosquatting* — prática que consiste em publicar bibliotecas com nomes semelhantes a pacotes legítimos e infectá-las com *malware*, na expectativa de que desenvolvedores desatentos as importem por engano.

O OWASP TOP 10:2025 evidencia avanços importantes na segurança oferecida pelos *frameworks* modernos, com impacto direto na redução de vulnerabilidades históricas. Mas também deixa claro que a superfície de ataque segue diretamente relacionada a decisões humanas. Falhas na lógica de autorização, más práticas no uso de dependências e erros por desconhecimento técnico demonstram que o desenvolvedor ainda é um agente central na segurança do ciclo de vida do *software*.

Em resumo, embora os *frameworks*, ferramentas, plataformas e metodologias de desenvolvimento de *software* tenham evoluído para oferecer mais segurança, a responsabilidade continua sendo compartilhada. É fundamental que as equipes de desenvolvimento incorporem boas práticas desde as etapas iniciais do ciclo de *software* — e compreendam que segurança não é apenas uma questão técnica, mas uma necessidade estratégica do negócio.

O OWASP TOP 10:2025 não apenas revela as vulnerabilidades mais exploradas nos últimos quatro anos, mas também convida o setor a repensar como o *software* é desenvolvido em um cenário cada vez mais complexo. Em vez de reagir a vulnerabilidades, a tendência é clara: prevenir desde o início, com arquitetura segura, equipes capacitadas e uma cultura de desenvolvimento responsável.

Martín Bedoya Rodriguez
Cybersecurity Expert Engineer



OWASP Top Ten 2025: do código seguro ao ecossistema seguro

Artigo por Evelyn Terrones Romero

A segurança no desenvolvimento de aplicações evoluiu de forma acelerada. O que antes era uma disciplina voltada à correção de falhas em código, hoje se transformou em uma gestão integrada de riscos que abrange todo o ecossistema de *software*. Este artigo analisa a evolução do OWASP Top Ten, destaca as principais novidades da edição 2025 e compara as mudanças mais relevantes em relação à versão anterior (2021), com o objetivo de entender melhor os riscos atuais e como nos preparar para mitigá-los.

OWASP Top Ten

O OWASP Top Ten é um projeto aberto e global que identifica as principais vulnerabilidades de segurança em aplicações, consolidando-se como padrão na gestão de riscos para desenvolvimento seguro. O foco do projeto está em riscos com alto impacto e frequência de exploração, tornando-se uma das referências mais influentes no campo da segurança em aplicações.

OWASP 2025: principais novidades

A versão OWASP Top Ten 2025, oitava desde seu lançamento em 2003, continua sendo o principal documento de referência global sobre os dez riscos mais críticos em aplicações web. Esta edição traz uma nova abordagem: embora mantenha a atenção sobre problemas estruturais, amplia o escopo para incluir riscos decorrentes do ambiente operacional, da cadeia de suprimentos de *software* e do tratamento de condições excepcionais.

O que inclui a nova versão 2025?

- Duas novas categorias
- Alterações nos nomes e escopos de várias categorias existentes
- Consolidação de riscos, agora agrupados por causa raiz e não apenas por sua manifestação técnica

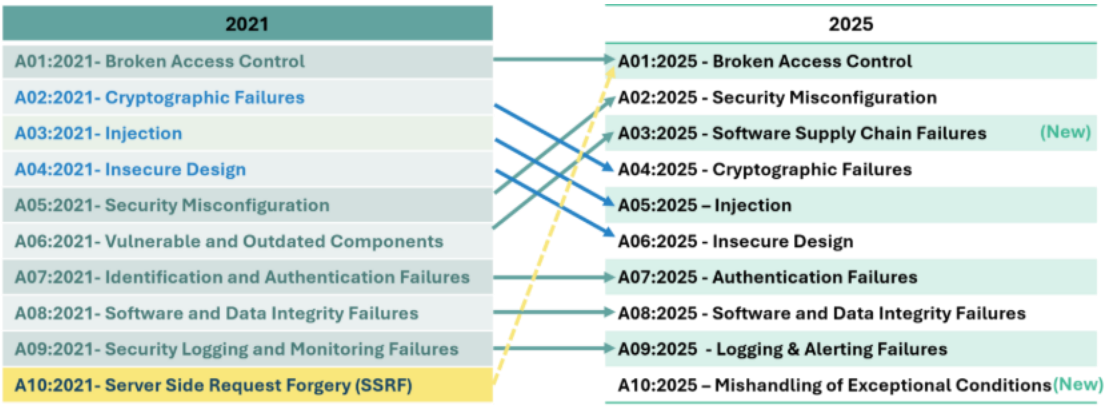
A seguir, as principais alterações desta nova edição:

A03: Falhas na cadeia de suprimentos de *software*

Este novo risco ocupa o terceiro lugar no ranking e substitui o antigo "Componentes vulneráveis e desatualizados" da edição de 2021. O escopo agora é mais amplo. Não se trata apenas do uso de bibliotecas inseguras, mas de todo o ecossistema de dependências — pacotes maliciosos, *scripts* comprometidos, *pipelines* vulneráveis e falhas na gestão de segredos. O foco está em reforçar a governança sobre terceiros.

A10: Tratamento inadequado de condições excepcionais

Essa nova categoria aborda falhas no tratamento de erros, *time-outs* não controlados, exceções mal gerenciadas, erros lógicos em estados anômalos e vazamento de informações sensíveis em mensagens de erro. Problemas antes considerados meramente operacionais passam agora a ser reconhecidos como vetores reais de ataque, capazes de expor dados confidenciais ou permitir execução maliciosa. Em 2025, o OWASP deixou claro que uma aplicação pode ser tecnicamente correta e ainda assim ser vulnerável se não responder de forma segura às ações inesperadas.



Fusão de SSRF com Quebra de Controle de Acesso

A vulnerabilidade conhecida como Server Side Request Forgery (SSRF), que anteriormente aparecia na categoria A10:2021, agora foi incorporada à nova A01:2025 – Quebra de Controle de Acesso.
Essa mudança reforça a compreensão de que o SSRF deve ser tratado como uma falha de controle de acesso — e não como uma vulnerabilidade isolada. Isso reforça o foco no acesso a recursos internos, APIs e serviços de *backend*, que atualmente representam vetores críticos de ataque em ambientes *cloud*.

Ascensão da categoria de Configuração Incorreta de Segurança

A categoria A05:2021 – Configuração Incorreta de Segurança sobe para a posição A02:2025, reconhecendo que muitos dos erros atuais não estão no código em si, mas sim na forma como os ambientes são configurados. Entre os exemplos comuns estão: credenciais padrão mantidas ativas, permissões mal definidas, serviços expostos, políticas inseguras ou ausência de cabeçalhos de segurança.

A injeção e as falhas criptográficas caem algumas posições

Essas categorias perdem posições no OWASP Top Ten 2025, não por redução de gravidade, mas porque o contexto atual apresenta outros riscos com maior frequência e impacto prático. Em outras palavras, o volume de exploração de outras vulnerabilidades cresceu mais rapidamente, alterando a prioridade de mitigação.

O que a nova edição nos ensina?

- **Segurança não é mais responsabilidade exclusiva da equipe de desenvolvimento:**

As novas categorias deixam claro que equipes de DevOps, infraestrutura e segurança devem atuar de forma integrada. Um código bem escrito, quando implantado em um ambiente mal configurado, continua sendo vulnerável.

- **Suas dependências são sua responsabilidade:**

É fundamental escanear e gerenciar dependências, monitorar vulnerabilidades conhecidas e aplicar princípios de confiança zero (zero trust) desde a concepção da aplicação.

- **Os erros também são portas de entrada para ataques:**

O novo foco no tratamento de exceções e condições inesperadas mostra que a resiliência de um sistema não é apenas operacional. Um erro mal gerenciado pode facilmente se transformar em uma vulnerabilidade — por isso, antecipar e controlar essas falhas deve ser parte essencial de qualquer estratégia de segurança eficaz.

O **OWASP Top Ten 2025** marca um novo estágio na maturidade da segurança em aplicações. Hoje, o risco não está apenas no código-fonte, mas em como integramos, implantamos, configuramos e operamos nossos *softwares*. Essa visão mais ampla exige uma cultura DevSecOps real, baseada na colaboração entre diferentes áreas.

Em um cenário de desenvolvimento acelerado, dependência de componentes externos e implantação contínua, conhecer e aplicar o OWASP Top Ten não é mais apenas uma boa prática — **é uma necessidade estratégica**.

Evelyn Terrones Romero
Cybersecurity Expert Analyst

A evolução do ecossistema OWASP

Tendências por Diego Carreño

O OWASP deixou de ser apenas aquela lista de vulnerabilidades que aparece em todo relatório de *pentest*. Hoje, tornou-se o sistema operacional silencioso da segurança do *software* moderno. Já não se trata apenas do Top 10, mas de um ecossistema de padrões — como ASVS, MASVS, SAMM, API Security, LLM Top 10, AI Testing Guide, entre outros— que orientam como projetamos, desenvolvemos, testamos e governamos aplicações, APIs e sistemas baseados em IA.

Falar de OWASP hoje é falar de um verdadeiro "sistema operacional" para a segurança de *software*. Um conjunto de normas, controles, boas práticas e metodologias que estruturam desde o planejamento de um *backlog* até as auditorias de compliance técnico. Não se trata apenas de proteger o código — mas de criar organizações que pensem, criem e protejam o *software* de forma integral.

De *checklist* a "sistema operacional" de AppSec

O primeiro grande indício dessa mudança foi o surgimento do OWASP ASVS (para aplicações web e serviços) e do MASVS (para apps mobile), que definem níveis de segurança (L1, L2, L3) e requisitos claros — mapeados em políticas, histórias de usuário, critérios de aceitação e escopos de teste. A partir disso, formou-se um ecossistema cada vez mais robusto:

- SAMM, como modelo de maturidade para programas de segurança de *software* com abordagem evolutiva;
- A Web Security Testing Guide (WSTG) e a Mobile Application Security Testing Guide (MASTG), como catálogos completos de testes que funcionam como *suites* de regressão para web e mobile;
- Guias como o Cheat Sheet Series e o Proactive Controls, que apresentam soluções específicas para codificação defensiva;
- O projeto Threat Modeling, com ferramentas como o Threat Dragon e abordagens como Cornucopia, que ajudam a antecipar riscos no *backlog* desde a fase de concepção;
- Ambientes de prática como o Juice Shop ou WebGoat, intencionalmente vulneráveis, utilizados para treinar equipes e validar regras de análise estática e dinâmica;
- Além dos Top 10 especializados, como o API Security Top 10, o Top 10 for LLM Applications, entre outros — que já estão moldando as metodologias de teste para sistemas com IA generativa.

A tendência é clara, as organizações deixaram de adotar esses projetos de forma isolada. Agora, os integram como módulos de um sistema coerente e transversal ao negócio.

O resultado prático? O OWASP deixa de ser uma lista consultada no fim do projeto para se tornar a camada estrutural desde a concepção até a entrada em produção.

OWASP como "linguagem comum" entre negócio, desenvolvimento e risco

Um dos avanços mais notáveis é o uso do OWASP como ponte de comunicação entre áreas que tradicionalmente falavam em "idiomas diferentes". Negócios operam com KPIs e riscos, desenvolvedores falam em *bugs* e dívida técnico, risco e compliance foca em controles e normas. O OWASP começa a atuar como um tradutor entre todos esses domínios. Alguns exemplos práticos que vimos em 2025:

- *Product owners*, junto com analistas de segurança, definem o nível de segurança-alvo de cada iniciativa com base no ASVS ou MASVS, e o incorporam como requisito não funcional no *backlog*;
- As áreas de risco e compliance mapeiam normas como PCI-DSS, NIS2 ou regulamentações locais em requisitos OWASP (ex: autenticação, *logging*, criptografia);
- A auditoria interna utiliza o SAMM para avaliar capacidades, *roadmap* e evidências de melhoria contínua — indo além de controles pontuais;
- Fábricas de software e equipes de *testing* padronizam histórias de usuário seguras, critérios de aceitação e casos de teste baseados no ASVS, WSTG, MASTG e Cheat Sheets.

O resultado é que uma conversa que costumava ocorrer em três idiomas diferentes começa a ter um dicionário em comum. Quando alguém diz "vamos elevar esta API para o nível ASVS L2 e cobrir o Top 10 de segurança para APIs", todos sabem o que isso significa — e o mais importante, como medir se está sendo cumprido.

OWASP como alicerce da automação

A outra grande alavanca de transformação é a automação. O OWASP passou a funcionar como taxonomia padrão para orquestrar *pipelines* de DevSecOps, correlacionar descobertas e priorizar a remediação de forma estruturada.

Ferramentas como SAST, DAST e IAST já identificam e classificam vulnerabilidades com base nas principais referências do OWASP — como ASVS, API Security Top 10 2023, Top 10 para LLMs, entre outras. Em muitas organizações, essas descobertas são consolidadas em um painel unificado de segurança de aplicações, estruturado segundo essa mesma taxonomia. A partir daí, os *pipelines* de CI/CD aplicam "perfis OWASP" personalizados, de acordo com o tipo da aplicação e seu nível de criticidade.

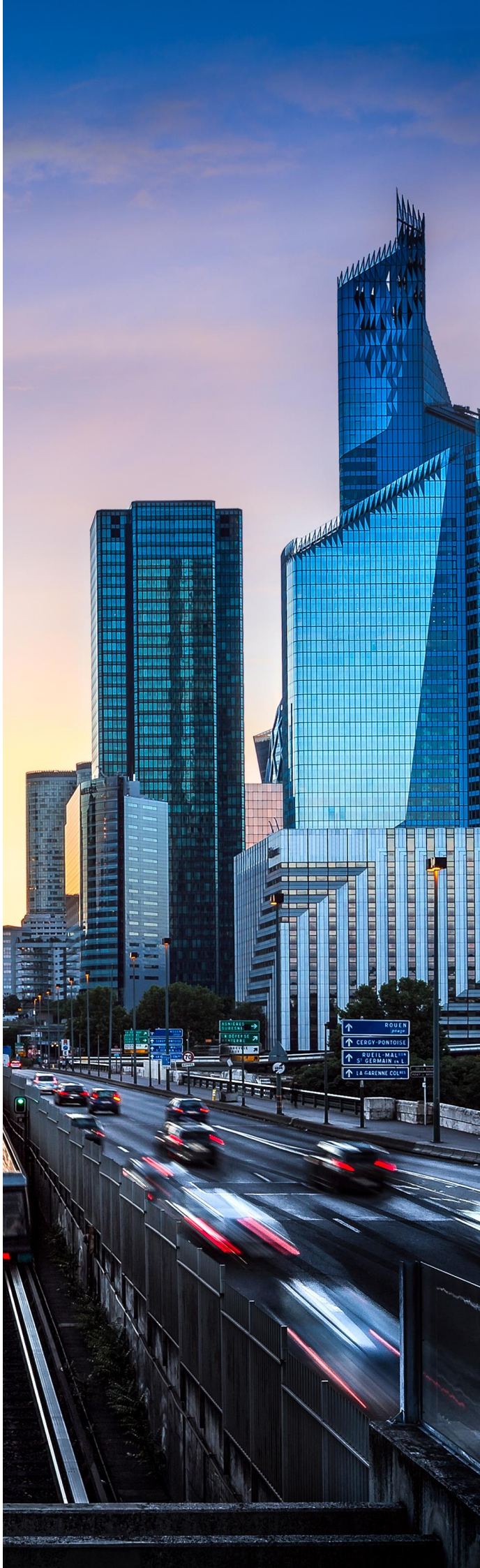
Inclusive, assistentes de IA Generativa voltados ao desenvolvimento seguro já estão sendo treinados com os padrões OWASP — como ASVS, MASVS, Cheat Sheets, WSTG, MASTG e o recém-lançado AI Testing Guide. Isso garante que, desde o primeiro comando gerado, as recomendações de design, codificação defensiva e testes já estejam alinhadas com os padrões mais reconhecidos do setor.

Conclusão: a próxima vantagem competitiva será ser fluente em OWASP

As organizações que adotarem essa tendência como uma decisão estratégica (e não como "apenas mais uma referência") serão aquelas capazes de alinhar negócios, desenvolvimento, risco e auditoria em uma única linguagem; industrializar controles e testes sem perder a rastreabilidade; e incorporar novas tecnologias sem precisar reinventar o modelo de segurança do zero a cada ciclo.

O OWASP, portanto, deixa de ser a referência que se consulta quando algo dá errado e passa a ser a camada estrutural que orienta como construir o que precisa dar certo. E isso, longe de ser uma tendência passageira, tem tudo para definir a próxima década do desenvolvimento seguro.

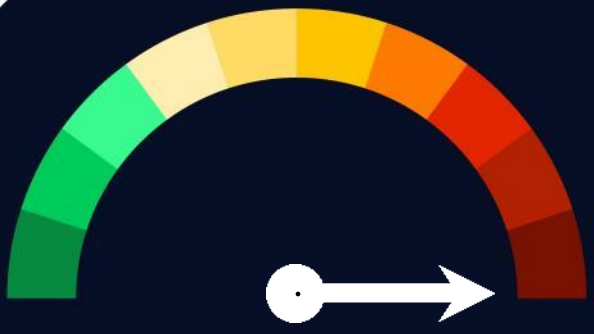
Diego Carreño
Cybersecurity Lead Analyst



Vulnerabilidades

Vulnerabilidade crítica em React Server Components

Data: 3 de dezembro de 2025
CVE: CVE-2025-55182



CVSS: 10

CRÍTICA

Descrição

Foi reportada uma vulnerabilidade de severidade crítica presente nas funções de servidor do React.

O React fornece ferramentas e integrações utilizadas por empacotadores e *frameworks* para executar código tanto no cliente quanto no servidor.

O React converte as requisições feitas pelo cliente em chamadas HTTP que são encaminhadas ao servidor. O servidor transforma essas chamadas em execuções de funções e retorna os resultados.

Um invasor não autenticado poderia elaborar uma requisição HTTP maliciosa direcionada a um servidor React, de modo que, ao ser traduzida, resulte na execução de código no sistema.

Solução

Recomenda-se atualizar imediatamente para as versões com correções aplicadas:

- React Server Components versões 19.0.1, 19.1.2 e 19.2.1.
- Caso a aplicação utilize o *framework* @vitejs/plugin-rsc, recomenda-se atualizar para @vitejs/plugin-rsc@0.5.3 ou versões posteriores.
- Para Next.js, as versões 15.x e 16.x devem ser atualizadas para: 15.0.5, 15.1.9, 15.2.6, 15.3.6, 15.4.8, 15.5.7 e 16.0.7.
- Para versões 14.3.0-canary.77 ou posteriores, recomenda-se retornar para a versão estável 14.x ou para 14.3.0-canary.76.

Produtos afetados

Alguns dos produtos afetados são:

- pacote web react-server-dom (react-server-dom-webpack;
- pacote DOM de servidor React (react-server-dom-parcel);
- react-server-dom-turbopack

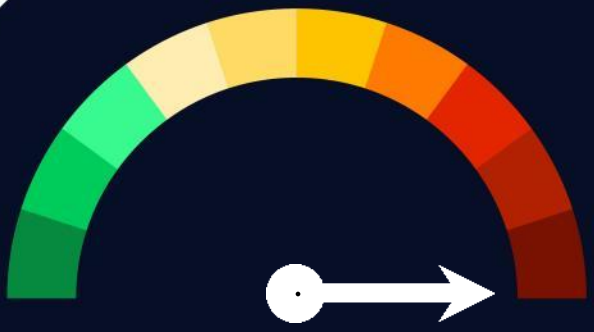
Referências

- nvd.nist.gov
- www.incibe.es

Vulnerabilidades

Vulnerabilidade crítica em Apache Tika

Data: 4 de dezembro de 2025
CVE: CVE-2025-66516



CVSS: 10

CRÍTICA

Descrição

Uma vulnerabilidade crítica de injeção XEE foi identificada em diversos componentes do Apache Tika.

Essa falha permite que um arquivo PDF manipulado com conteúdo XFA malicioso provoque o carregamento de entidades XML externas durante o processamento. Isso resulta na exposição de arquivos do sistema, o que, em determinados ambientes, pode facilitar ataques de maior gravidade.

A vulnerabilidade amplia o alcance da falha previamente identificada (CVE-2025-54988), pois também afeta módulos adicionais e versões do Tika em que o código vulnerável estava localizado em pacotes internos distintos, dificultando sua detecção.

Solução

Recomenda-se atualizar imediatamente as versões afetadas para as versões com correções aplicadas:

- Tika-core: versão 3.2.2
- Tika-parser-pdf-module: versão 3.2.2
- Tika-parsers: versão 2.0.0

Produtos afetados

Os pacotes afetados incluem as versões:

- Tika-core: versões 1.13 a 3.2.1
- Tika-parser-pdf-module: versões 2.0.0 a 3.2.1
- Tika-parsers: versões 1.13 até anteriores à 2.0.0

Referências

- thehachernews.com
- incibe.es

Android corrige 107 vulnerabilidades em seu patch de segurança de dezembro

Fecha: 1 de diciembre de 2025
CVE: CVE-2025-48631 e outras 106

Crítica

Descrição

O Android publicou o patch de segurança referente ao mês de dezembro, no qual corrige um total de 107 vulnerabilidades. Dentre elas, há 7 vulnerabilidades de severidade crítica e 98 de severidade alta.

O fabricante informou que há indícios de exploração ativa das vulnerabilidades CVE-2025-48572 e CVE-2025-48633.

A primeira pode permitir que um hacker realize uma escalação de privilégios, enquanto a segunda corresponde a uma vulnerabilidade de divulgação de informações.

Entre as vulnerabilidades, destaca-se a crítica CVE-2025-48631, localizada no componente *framework*, que pode permitir um ataque remoto de negação de serviço, sem a necessidade de privilégios adicionais.

Produtos afetados

Os produtos afetados pela atualização são:

- Android Open Source Project (AOSP): versões 13, 14, 15 e 16
- Componentes da Arm, MediaTek, Unisoc e Qualcomm

Solução

Recomenda-se aplicar os patches de segurança publicados pelo fabricante.

Referências

- source.android.com
- incibe.es

Sneeit Framework corrige uma vulnerabilidade de execução remota de código (RCE)

Fecha: 8 de diciembre de 2025
CVE: CVE-2025-6389

Crítica

Descrição

Foi identificada uma vulnerabilidade crítica no Sneeit Framework, um componente amplamente utilizado por diversos temas e templates premium do WordPress.

A vulnerabilidade permite que um atacante remoto não autenticado execute funções PHP arbitrárias por meio de uma chamada manipulada ao *framework*.

A falha está localizada em uma função que processa entradas de usuários sem validação, o que possibilita a execução de funções arbitrárias no servidor, podendo resultar em instalação de *backdoors*, criação de contas administrativas não autorizadas ou comprometimento de sites.

Produtos afetados

Os produtos afetados pela atualização são:

- Todas as versões do Sneeit Framework até a 8.3, inclusive
- Qualquer tema ou template WordPress que incorpore essa versão do *framework*

Solução

O desenvolvedor recomenda:

- atualizar para o Sneeit Framework 8.4;
- revisar configurações, contas administrativas e possíveis indícios de comprometimento.

Referências

- techradar.com
- nvd.nist.gov

Eventos

NIST Small Business Cybersecurity Webinar
20 de janeiro

O NIST oferecerá um webinar virtual, por meio da plataforma Zoom for Government, com foco em ajudar pequenas e médias empresas a proteger informações não classificadas controladas *(Controlled Unclassified Information — CUI)*. Durante a sessão, será apresentado o novo documento "Small Business Primer" da SP 800-171 Revisão 3, com explicações sobre seus principais requisitos. Especialistas do NIST orientarão sobre como começar a implementar essas práticas de segurança e responderão às dúvidas dos participantes.

Link

II Jornada DORA
21 de janeiro

Evento de referência para compartilhamento de experiências, avaliação de avanços e discussão de desafios regulatórios ligados à regulamentação DORA (Digital Operational Resilience Act). A programação contará com mesas-redondas formadas por representantes dos principais agentes envolvidos na norma, entre eles reguladores, CISOs e autoridades públicas. Está confirmada a participação de representantes do Ministério para a Transformação Digital e da Função Pública, INCIBE, Agência de Cibersegurança de Madri, Banco de España, Banco Santander, BBVA, CaixaBank, Mapfre, ING Bank, Allianz, Abanca, Sabadell Digital, Bankinter Group, Unicaja, Singular Bank, Santalucía, AXA Seguros e Triodos Bank.

Link

IA Expo Internacional 2026
31 de janeiro

A IA Expo Internacional 2026 será realizada em 31 de janeiro de 2026, no hotel The Westin Santa Fe, na Cidade do México. O evento reunirá líderes, empreendedores, desenvolvedores, pesquisadores e executivos para discutir casos reais de adoção de inteligência artificial, suas aplicações práticas em diversos setores, além de temas essenciais como ética, segurança, automação, transformação digital e inovação com IA.

Link

Recursos

➢ Melhores práticas para higienização de mídia

O NIST, por meio da publicação “Melhores práticas para higienização de mídia” (NIST Special Publication 800-88 Revision 1), estabelece uma estrutura técnica específica e padronizada para a sanitização segura de mídias de armazenamento, com o objetivo de garantir que informações sensíveis sejam eliminadas de forma eficaz e não possam ser recuperadas por agentes não autorizados.

O documento descreve métodos de limpeza lógica, depuração e destruição física aplicáveis a diferentes tipos de dispositivos (HDD, SSD, USB, equipamentos móveis, fitas, etc.), fornece critérios para selecionar a técnica adequada com base no nível de sensibilidade dos dados e no ciclo de vida do meio, e define responsabilidades organizacionais para assegurar uma gestão segura e rastreável.

Link

➢ NIST Investments 2025

O relatório “NIS Investments 2025”, publicado pela ENISA, analisa em detalhes como os Estados-membros da União Europeia e os operadores de serviços essenciais estão investindo em capacidades de cibersegurança para atender aos requisitos da Diretiva NIS2 e reforçar sua resiliência às crescentes ameaças digitais. O relatório apresenta dados e tendências sobre prioridades de investimento, nível de maturidade das capacidades nacionais, evolução dos riscos, além dos desafios regulatórios e operacionais enfrentados pelo ecossistema europeu.

Link

Inscreva-se na RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

br.nttdata.com