Número 107 | Outubro de 2025

NTT DATA

Radar

A sua revista de cibersegurança

A identidade é a nova zona de "máxima segurança"

Por Hans Vigil Navas

Se 2024 foi o ano da consolidação do Zero Trust, 2025–2026 serão os anos em que a identidade será operacionalizada como o verdadeiro perímetro de segurança. Três forças puxam esse movimento: a maturidade das diretrizes do NIST sobre identidade digital, a pressão das APIs como espinha dorsal dos negócios e a profissionalização dos ataques contra fatores fracos de autenticação.

Na nossa região (marcada por ecossistemas multicloud, serviços públicos digitais em expansão e cadeias de fornecimento cada vez mais baseadas em SaaS) o custo de não modernizar o IAM deixou de ser técnico: virou estratégico.

1. Do "cumprir MFA" à autenticação resistente a *phishing*

O NIST publicou em agosto de 2025 a revisão 4 do SP 800-63, atualizando os requisitos de verificação de identidade, autenticação e federação, incorporando também aspectos de privacidade e experiência do usuário. Para os CISOs, isso significa elevar a régua para MFA resistente a *phishing* e padronizar níveis de garantia em toda a jornada digital, desde o *onboarding* até a recuperação e a federação com terceiros.

2. *Passwordless* de verdade (e com métricas)

O avanço global das *passkeys* (FIDO2/WebAuthn) deixou de ser promessa: já são mais de 15 bilhões de contas aptas a usá-las, e a adoção corporativa cresce, apoiada em guias e métricas públicas da FIDO Alliance. Em 2025, quase metade dos 100 sites mais acessados já suportava a tecnologia. Para a América Latina, isso implica planejar migrações graduais, políticas claras de recuperação e portabilidade, além de educação dos usuários para reduzir fricções.

3. Zero Trust aplicado à identidade

Os documentos NIST SP 800-207 e 800-207A reposicionam os controles para decisões contínuas e contextuais de acesso, desacoplando rede e recurso. Na prática, isso pede políticas no nível da aplicação, sinais de postura do dispositivo e reautenticação adaptativa. O objetivo não é "fechar a rede", mas autorizar cada solicitação com base em contexto atualizado.

4. APIs: onde o controle de acesso se perde (ou se consolida)

Enquanto o OWASP Top 10 para aplicações web ainda aponta o Broken Access Control como risco crítico, o OWASP API Security Top 10 (2023) mostra que as falhas mais exploradas são BOLA/BOPLA e autenticação quebrada.

Para 2025–2026, a recomendação é clara: *policy-as-code* para autorização em nível de objeto/propriedade, inventário e classificação de APIs, testes de segurança no pipeline e governança de tokens (rotação, escopos mínimos e detecção de uso anômalo).

5. ISO/IEC 27001:2022 como âncora de gestão

O padrão vigente continua sendo a ISO/IEC 27001:2022 (com emenda em 2024), que alinha controles à realidade da nuvem e da identidade. Para os CISOs, é a base para integrar IAM a risco, auditoria e gestão de fornecedores, evitando que seja visto apenas como "tecnologia" em vez de processo e melhoria contínua.

6. Novos desafios: máquinas, agentes e detecção de ameaças de identidade

A explosão de identidades não humanas (*workloads*, contêineres, chaves de serviço e agentes de IA) exige visibilidade, emissão *just-in-time*, *Zero Standing Privilege* e rotação automatizada. O mercado já reconhece o ITDR (Identity Threat Detection & Response) como categoria necessária para identificar abuso de tokens, "*impossible travel*", sequestro de sessões e "*consent phishing*".

Prioridades práticas para os próximos 12–18 meses

- Fortalecer a autenticação: implementar *passkeys* em aplicativos críticos, MFA resistente a *phishing* e recuperação sem SMS; medir adoção e sucesso por coortes.
- Governar acesso em APIs: inventário unificado, testes de autorização no CI/CD, escopos mínimos por cliente; telemetria de tokens e revogação em tempo real.
- Zero Trust "*identity-first*": políticas dinâmicas com sinais de dispositivo, localização e risco; revalidação contínua de sessões e privilégios.
- IAM não humano: emissão de credenciais efêmeras, rotação automática e registro criptográfico de uso; guardrails específicos para agentes de IA.

- Aderência à ISO 27001:2022: KPIs de IAM no ISMS, auditorias em terceiros (federação, IDaaS) e gestão de riscos de identidade pelo comitê de segurança.

- ITDR: detecção de anomalias centrada em identidade e *kill-switch* para tokens/sessões comprometidas, integrado ao SOC.

Por fim, modernizar o Identity & Access Management (IAM) não é um projeto, é um modelo operacional de negócio.

Adotar o NIST SP 800-63-4, fortalecer APIs segundo OWASP e ancorar a governança na ISO/IEC 27001:2022 permitirá às organizações do Peru e da América Latina sustentar o crescimento digital, atender regulações e reduzir riscos de fraude, invasão e abuso de privilégios de forma mensurável em 2025–2026.

Hans Vigil Navas
Gerente de Cibersegurança

Identidade digital: a chave mestra

Cibercrônica por Marlon Santiago Nivia Devia

Entre meados de 2024 e agosto de 2025, o cenário de cibersegurança deixou claro: até as organizações mais preparadas podem ruir se a gestão de identidades e acessos (IAM) for comprometida. Mais que um firewall ou antivírus, a identidade digital virou a chave mestra para infiltração, escalada de privilégios e comprometimento de infraestruturas críticas. Em menos de um ano, ataques em cadeia mostraram que a fraqueza não está sempre no código, mas muitas vezes nas credenciais, nos tokens e nas pessoas que os administram.

O primeiro grande sinal de alarme ocorreu em meados de 2024, quando o grupo ShinyHunters conduziu um dos maiores roubos de dados dos últimos tempos. Usando credenciais roubadas por *infostealers*, eles acessaram contas de clientes da Snowflake que não tinham autenticação multifator. O ataque foi silencioso e preciso: cruzaram credenciais comprometidas de máquinas infectadas, testaram acessos contra a nuvem da Snowflake e, já dentro, baixaram bancos de dados inteiros sem disparar alertas críticos.

Sem explorar falhas de código nem corromper colaboradores internos, bastou a ausência de um segundo fator de autenticação para abrir a porta. O resultado: milhões de registros de empresas como Ticketmaster, Santander, Advance Auto Parts, LendingTree e AT&T expostos. A extensão foi tanta, que boa parte desses dados acabou circulando em fóruns clandestinos como o BreachForums, onde foi revendida e trocada entre diferentes grupos criminosos. Esse episódio escancarou tanto o poder dos *infostealers* quanto a fragilidade de provedores externos que concentram informações críticas sem exigir autenticação reforçada.

Enquanto a indústria ainda digeria esse impacto, em dezembro de 2024 o alarme soou no coração do governo dos EUA. O Departamento do Tesouro sofreu o que chamou de seu "maior incidente de cibersegurança", atribuído a um APT possivelmente ligado ao Estado chinês. Explorando duas falhas zero-day no serviço de suporte da BeyondTrust, provedora de gestão de acesso privilegiado (PAM), os atacantes comprometeram a rede e roubaram uma chave de API com privilégios amplos. Com ela, redefiniram senhas de contas críticas e conseguiram acesso remoto a estações de trabalho com dados sensíveis sobre operações financeiras e políticas de sanções.

Apesar de a BeyondTrust ter revogado rapidamente a credencial comprometida e desligado instâncias suspeitas, ficou claro que, em IAM e PAM, um único token mal protegido pode virar a chave para todas as portas. O ataque também ganhou contornos políticos: enquanto os EUA acusavam formalmente a China, Pequim negava qualquer envolvimento, levando o caso para o campo da diplomacia.

Sem tempo de respirar, em abril de 2025, os varejistas britânicos Marks & Spencer e Co-op se viram no centro de um "evento cibernético combinado", segundo o Cyber Monitoring Centre. Com poucos dias de intervalo, o mesmo grupo aplicou ataques quase idênticos — não com *exploits* sofisticados, mas recorrendo à engenharia social. Fingindo ser funcionários de TI em chamadas e e-mails internos falsificados, enganaram equipes de help desk para resetar credenciais com privilégios administrativos. Com o acesso concedido, comprometeram sistemas internos de logística, inventário e vendas, causando interrupções e vazamento de dados comerciais.

O impacto foi profundo: dois alvos principais gravemente atingidos e um efeito dominó em fornecedores e parceiros dependentes dessas cadeias de suprimento. Pouco depois, o Google Threat Intelligence Group alertou que o grupo Scattered Spider replicava a mesma técnica contra seguradoras nos EUA, confirmando que o modelo era lucrativo e difícil de conter.

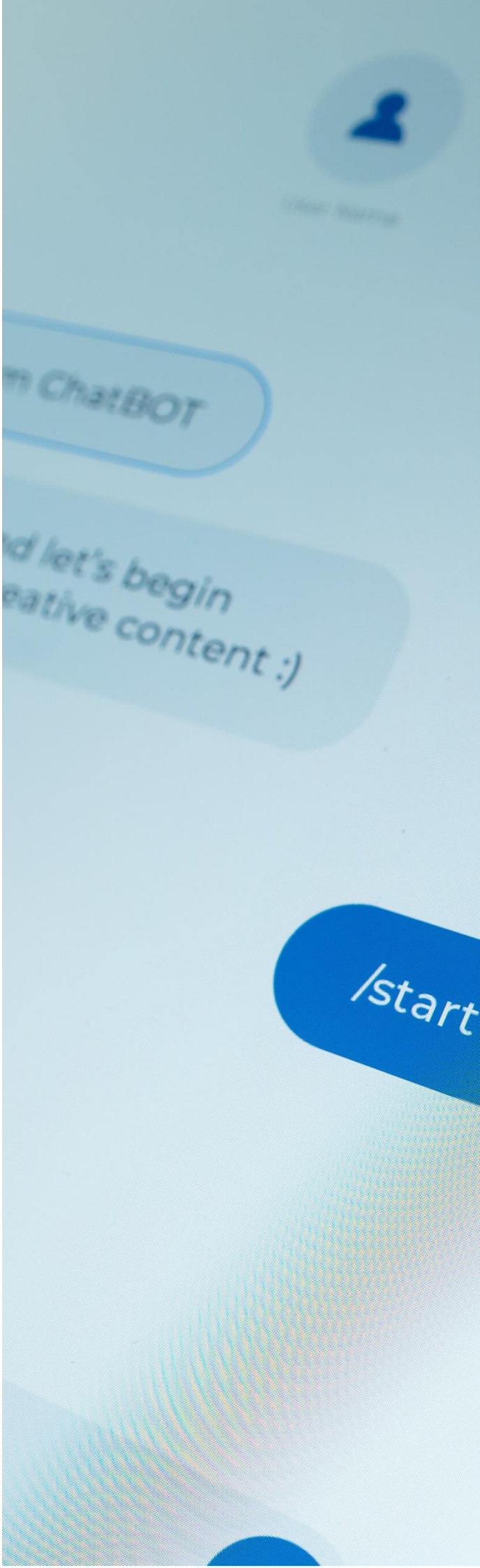
E quando parecia que o ano já tinha ensinado o suficiente, em agosto de 2025 a Cisco entrou na lista de vítimas. Dessa vez, o ataque não se apoiou em vulnerabilidades de software, mas em persuasão humana. Um golpe de *vishing* — *phishing* por voz — com múltiplas ligações, construção de confiança e um roteiro cuidadosamente elaborado, que convenceu um atendente de suporte a liberar acesso a um CRM externo.

Além disso, sistemas de IA podem aprender com incidentes passados, melhorando continuamente sua capacidade de reconhecer novas ameaças e reduzindo falsos positivos. Isso se traduz em respostas mais rápidas e eficazes, já que a IA consegue priorizar alertas e sugerir ações corretivas.

Por fim, essas técnicas facilitam a integração de múltiplas fontes de informação, oferecendo uma visão mais ampla do panorama de ameaças e ajudando analistas a tomar decisões mais embasadas.

No conjunto, essas capacidades tornam os SOCs mais proativos e eficientes na defesa contra ciberataques.

Marlon Santiago Nivia Devia
Analista Júnior de Cibersegurança



CIAM: Segurança e Experiência do Cliente na Era Digital

Por Alicia Lara Herrera

Em um cenário onde a experiência do cliente é tão importante quanto a segurança digital, o Customer Identity and Access Management (CIAM) se consolidou como um pilar essencial para organizações que querem oferecer serviços personalizados, seguros e eficientes. Diferente do Identity and Access Management (IAM) tradicional, voltado para colaboradores e recursos internos, o CIAM foca na gestão da identidade de milhões de clientes externos, equilibrando segurança, escalabilidade e experiência do usuário.

IAM x CIAM: compreendendo as diferenças

O IAM corporativo foi projetado para controlar o acesso de colaboradores, parceiros e dispositivos a sistemas internos de uma organização, priorizando eficiência operacional, conformidade regulatória e gestão de privilégios internos.
Já o CIAM é voltado para o cliente final. Suas prioridades são usabilidade, escalabilidade, segurança e conformidade com legislações de proteção de dados (como o GDPR). Além disso, agrega recursos como login social, gestão de consentimento, personalização da experiência e suporte a múltiplos canais (web, mobile, totens, etc.).

A Importância Estratégica do CIAM para as Empresas

Com a digitalização acelerada, os clientes interagem por aplicativos, portais, redes sociais e centrais de atendimento. Nesse contexto, gerenciar identidades de forma eficaz se tornou uma vantagem competitiva. Para além de uma mera camada de segurança, o Customer Identity and Access Management (CIAM) é uma plataforma estratégica que impacta diretamente a experiência do cliente, a conformidade regulatória, a eficiência operacional e o crescimento do negócio.

1. Experiência do Cliente (CX) Sem Atrito

Quando bem implementado, o CIAM permite aos usuários:

- Registro rápido e seguro;
- Login via identidade social (Google, Apple, Facebook, etc.);
- Autenticação sem senha (*passwordless*);
- Gestão de perfil, privacidade e consentimento via autoatendimento.

Isso se traduz em interações mais ágeis, menor taxa de abandono durante os processos de cadastro e maior fidelidade. No contexto atual, em que os clientes esperam uma experiência fluida e personalizada, o CIAM torna-se um facilitador fundamental.

2. Segurança e Confiança

Com o aumento das fraudes digitais, roubo de identidade e violações de dados, a cibersegurança se tornou uma prioridade crítica. O CIAM entrega:

- Autenticação multifator (MFA) robusta;
- Detecção de anomalias e inteligência comportamental para identificar acessos suspeitos;
- Gestão de sessões e revogação de tokens em tempo real.

Proteger a identidade de um cliente também significa proteger a reputação de uma empresa. Um incidente de segurança pode levar à perda de confiança, danos à reputação e sanções regulatórias.

3. Conformidade Regulatória

As estruturas regulatórias atuais exigem um controle rigoroso sobre:

- Consentimento explícito do usuário.
- Rastreabilidade e segurança dos dados pessoais.

Um CIAM moderno inclui ferramentas nativas para gerenciar o consentimento, registrar auditorias e permitir que os clientes exerçam seus direitos de forma autônoma.

4. Dados Confiáveis para Análise

O CIAM é a porta de entrada para dados valiosos sobre o comportamento do cliente: De onde eles acessam? Quais dispositivos eles usam? Com que frequência eles fazem login? Quais canais eles preferem?

Pontos-chave da jornada do cliente

Ao longo do ciclo de vida do cliente, o CIAM intervém em momentos críticos:

1) **Registro:** integração de opções como login social, e-mail e SMS. Captura de consentimento.
2) **Autenticação:** autenticação segura usando MFA, biometria ou autenticação adaptativa.
3) **Gestão de identidade:** autoatendimento para atualização de dados e preferências de privacidade.
4) **Acesso a recursos:** autorização baseada em funções, atributos ou políticas.
5) **Logout e Revogação:** mecanismos seguros para logout e revogação de tokens.

Protocolos de Autenticação e Autorização

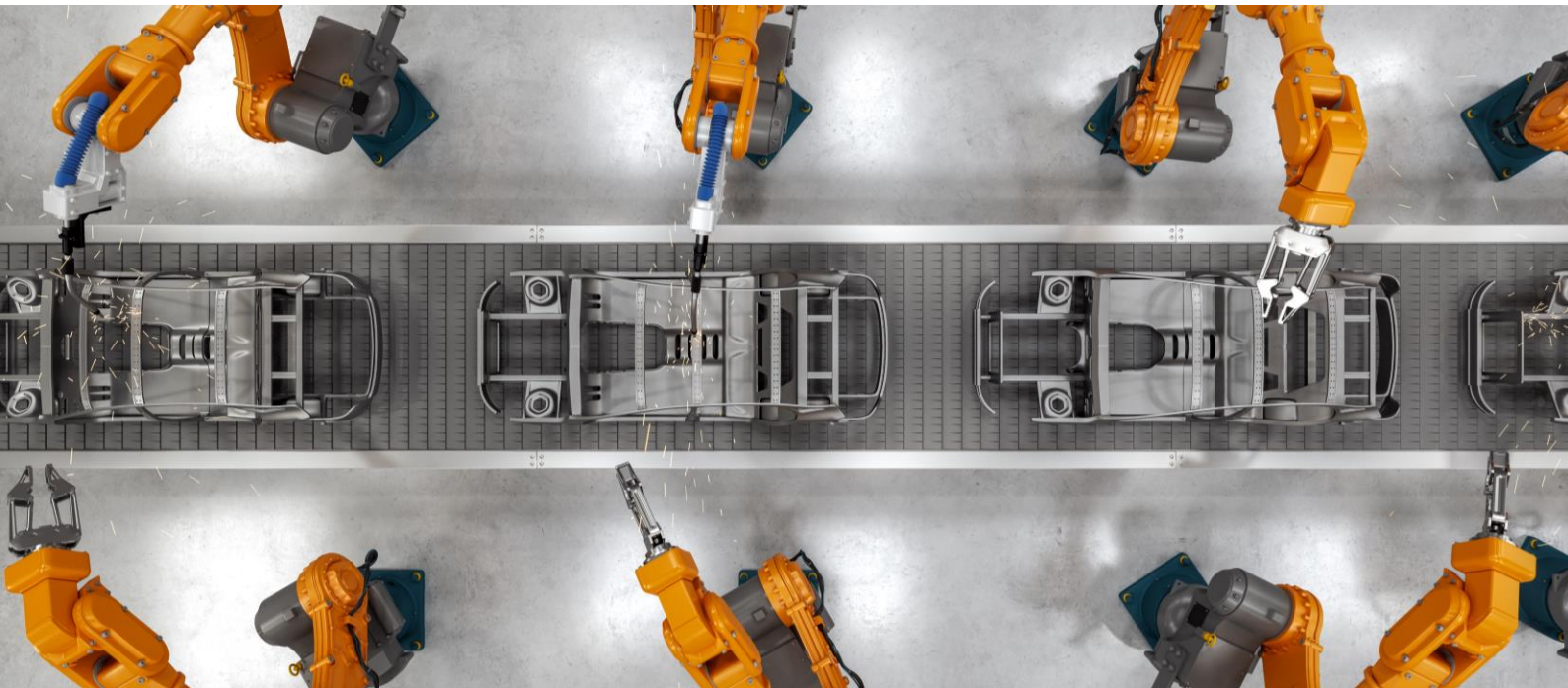
O CIAM baseia-se em padrões abertos para garantir interoperabilidade, segurança e escalabilidade:

- OAuth 2.0: Protocolo de autorização que permite que aplicativos acessem recursos em nome do usuário sem compartilhar credenciais. Seus principais recursos incluem:
  - Delegação de acesso
  - Suporte para tokens de acesso de curta duração
  - Adoção em APIs e serviços modernos.
  - OpenID Connect (OIDC): Estende o OAuth 2.0 para incorporar autenticação. Permite que aplicativos conheçam a identidade do usuário, obtendo informações adicionais por meio de um ID Token (JWT).
- JSON Web Token (JWT): Formato compacto e seguro que transporta informações entre as partes como tokens de autenticação ou autorização. Inclui declarações assinadas digitalmente e, em alguns casos, criptografadas.

Em resumo, a adoção de um CIAM moderno não apenas fortalece a cibersegurança de uma organização, mas também melhora radicalmente a experiência do cliente. Integrar autenticação forte, gerenciamento de consentimento, padrões abertos e uma abordagem centrada no usuário é essencial para competir em um ambiente digital cada vez mais exigente.

Nesse sentido, o CIAM é mais do que uma tecnologia: é um facilitador essencial do crescimento, da confiança e da inovação empresarial.

Alicia Lara Herrera
Engenheira Especialista em Cibersegurança



O Mundo PAM (Privileged Access Management)

Por Mijail Muñoz Loja

No contexto da cibersegurança, poucos riscos são tão críticos quanto o mau gerenciamento de acessos privilegiados, uma vez que usuários com permissões elevadas conseguem acessar informações críticas e sistemas sensíveis que, se caírem em mãos erradas, podem causar danos irreversíveis. O **Privileged Access Management (PAM)** é um conjunto de políticas, ferramentas e práticas de segurança desenvolvidas para controlar, monitorar e auditar acessos privilegiados, visando minimizar os riscos relacionados a estes acessos tão sensíveis. O PAM desempenha um papel fundamental na proteção da infraestrutura digital de uma organização, garantindo que os privilégios sejam concedidos e utilizados adequadamente.

1. O que é Privileged Access Management (PAM)?

PAM refere-se às estratégias e ferramentas implementadas para gerenciar, proteger, monitorar e auditar os acessos privilegiados dentro de uma organização. Acesso privilegiado é aquele que concede a um usuário, administrador ou aplicativo a capacidade de executar tarefas críticas, como configuração do sistema, gerenciamento de banco de dados ou controle de rede e servidor. Essas contas podem causar mudanças significativas no ambiente de TI e, portanto, o gerenciamento inadequado delas pode se tornar a porta de entrada perfeita para ataques cibernéticos.
O principal objetivo do PAM é limitar, gerenciar e monitorar o acesso a recursos críticos, garantindo que os usuários tenham apenas os privilégios necessários para executar suas tarefas e que esses acessos sejam constantemente monitorados e auditados para detectar qualquer atividade suspeita. (CyberArk, n.d.) (Fortinet, n.d.) (Techopedia, n.d.)

2. O Tamanho do Mercado de PAM

i. Tamanho e Perspectivas do Mercado Global de Gerenciamento de Acesso Privilegiado

O tamanho do mercado global de gerenciamento de acesso privilegiado foi estimado em US$ 3.285,7 milhões em 2024 e a projeção é de que atinja US$ 9.385,6 milhões até 2030, crescendo a uma CAGR de 19,7% entre 2025 e 2030. O aumento das ameaças à cibersegurança, incluindo vazamentos de dados e ataques internos, tem levado as organizações a adotar práticas mais robustas de gerenciamento de acesso. Requisitos regulatórios rigorosos e normas de conformidade, como GDPR e HIPAA, aceleram ainda mais a necessidade por sistemas seguros. (Global, n.d.)

Mercado Global de Gerenciamento de Acesso Privilegiado, 2018-2030 (US$ M)

Destaques do Mercado Global de Gerenciamento de Acesso Privilegiado

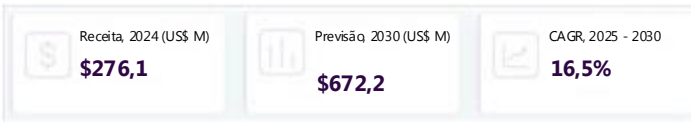
- Espera-se que o mercado cresça a uma CAGR (2025-2030) de 19,7% até 2030.
- Em termos de segmento, o software de gerenciamento de acesso privilegiado foi responsável por uma receita de US$ 2.407,2 milhões em 2024.
- O software de gerenciamento de acesso privilegiado é o segmento mais lucrativo, registrando o crescimento mais rápido durante o período previsto.
- Em termos de região, a América do Norte foi o maior mercado gerador de receita em 2024.
- Em termos de países, espera-se que a Coreia do Sul registre o maior CAGR de 2025 a 2030.

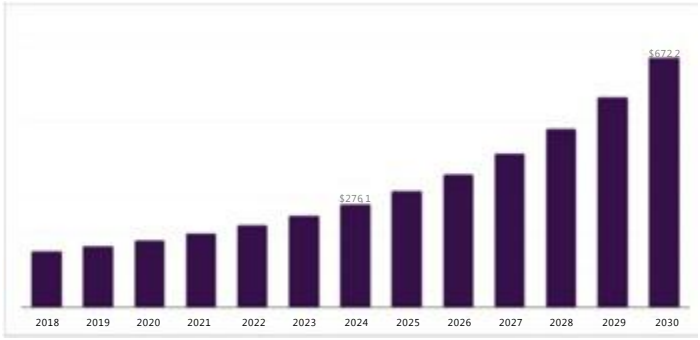
Outras Tendências Importantes do Setor

Em termos de receita, a América do Norte foi responsável por 35,1% do mercado global de gerenciamento de acesso privilegiado em 2024. Por país, projeta-se que os EUA liderem o mercado global em termos de receita em 2030. A Coreia do Sul é o mercado regional de crescimento mais rápido e a projeção é de atingir US$ 326,7 milhões até 2030. (Global, n.d.)

ii. Tamanho e Perspectivas do Mercado de Gerenciamento de Acesso Privilegiado na América Latina

Espera-se que o mercado de gerenciamento de acesso privilegiado na América Latina atinja uma receita projetada de US$ 672,2 milhões até 2030. Além disso, espera-se que o mercado de gerenciamento de acesso privilegiado na América Latina registre uma taxa de crescimento anual composta de 16,5% entre 2025 e 2030. (Latam, n.d.)





Mercado Latino-Americano de Gerenciamento de Acesso Privilegiado, 2018-2030 (US$ M)

Destaques do Mercado Latino-Americano de Gerenciamento de Acesso Privilegiado

- O mercado latino-americano de gerenciamento de acesso privilegiado gerou uma receita de US$ 276,1 milhões em 2024.
- Espera-se que o mercado cresça a uma CAGR de 16,5% entre 2025 e 2030.
- Em termos de segmento, o software de gerenciamento de acesso privilegiado foi o tipo que mais gerou receita em 2024.
- O software de gerenciamento de acesso privilegiado é o segmento mais lucrativo, registrando o crescimento mais rápido durante o período previsto.
- Em relação ao país, espera-se que o Brasil registre o maior CAGR entre 2025 e 2030. (Latam, n.d.)

3. Benefícios da Implementação do PAM

A implementação de uma solução PAM em uma organização trará diversos benefícios importantes para a segurança:

- Redução dos riscos de acesso não autorizado;
- Minimização de danos potenciais em caso de comprometimento;
- Conformidade regulatória;
- Melhor visibilidade e controle sobre as atividades do administrador.
- Automação dos processos de gerenciamento de contas.

4. Conclusão

O gerenciamento de acesso privilegiado (PAM) é um elemento essencial em qualquer estratégia moderna de cibersegurança. Considerando o grande número de ataques focados em contas privilegiadas, sua implementação correta reduz significativamente os riscos e garante a proteção da infraestrutura crítica da organização.

Com o crescimento das ameaças e a complexidade crescente do ambiente digital, adotar o PAM deixou de ser uma opção e se tornou uma necessidade para proteger os ativos mais importantes de qualquer organização.

Mijail Muñoz Loja
Engenheiro Chefe de Cibersegurança

Baterias Quânticas

Espaço Quântico por María Gutiérrez

A transição energética depende de um elemento essencial: as baterias. De celulares a veículos elétricos, incluindo redes inteligentes, o armazenamento de energia eficiente e seguro é um desafio fundamental. No entanto, compreender e aprimorar baterias exige adentrar um campo em que a física clássica (o mundo dos elétrons e das interações químicas) começa a ficar aquém do esperado, enquanto a computação quântica emerge como uma ferramenta transformadora.

O limite da simulação clássica

Atualmente, pesquisadores utilizam a química computacional e a dinâmica molecular para prever o comportamento dos materiais das baterias. Esses métodos permitem, por exemplo, estimar como um íon de lítio se move através de um eletrólito ou como uma molécula reage no cátodo. Mas à medida que a complexidade aumenta — como ocorre na formação da chamada interface sólido-eletrólito (SEI), que determina a vida útil da bateria — os algoritmos clássicos tornam-se proibitivamente demorados e dispendiosos. O problema torna-se intrínseco: simular com precisão os estados eletrônicos de um sistema cresce exponencialmente com o número de partículas.

O salto quântico. A bateria de Dicke

A computação quântica promete superar essa barreira, com computadores capazes de abordar diretamente problemas que exigem aproximações em um sistema clássico. No caso específico das baterias, e devido à sua viabilidade experimental, a equipe da NTT DATA propôs um projeto de pesquisa focado na bateria de Dicke, que se destaca como um dos conceitos mais promissores em termodinâmica quântica e tecnologia de armazenamento de energia.

O projeto se baseia no modelo de 1954 de Robert Dicke, que descreve como um conjunto de átomos ou emissores quânticos (como qubits, íons ou moléculas) interage coletivamente com um campo eletromagnético. Em vez de agirem de forma independente, os átomos se acoplam coletivamente, de maneira semelhante à radiação, podendo gerar fenômenos como a “superradiância”: todos descarregam sua energia de forma sincronizada, muito mais rápido do que fariam isoladamente. Traduzida para baterias, a ideia é carregar e descarregar energia de forma quântica, coletiva e ultrarrápida.

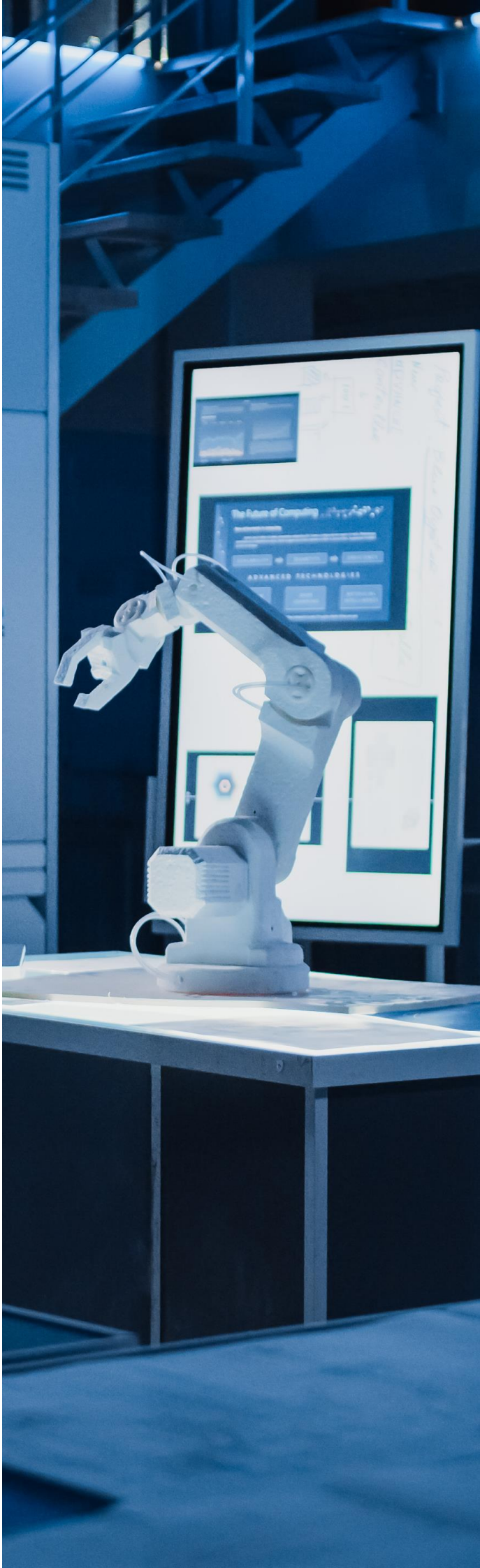
O projeto de pesquisa da NTT DATA utiliza aprendizado por reforço (RL) para otimizar o processo de carregamento de uma bateria Dicke, com foco no desenvolvimento do algoritmo de função política de um agente de RL utilizando algoritmos de otimização quântica aproximada (QAOA). Ele verifica se a energia extraível (ergotropia) e as flutuações da energia mecânica quântica (precisão de carregamento) podem ser melhoradas em comparação com estratégias de carregamento padrão. O estudo também incluirá uma análise do mapa de valor com base nas estratégias utilizadas, comparando-as com sua "verdade fundamental". Este último visa quantificá-lo em nível empresarial para verificar seu impacto econômico.

Quais os benefícios que isso traz?

Estes ainda são protótipos de laboratório em pequena escala (dezenas de qubits no máximo). Não existe uma bateria Dicke operacional no sentido clássico (armazenamento e recuperação de energia elétrica para dispositivos).

O que foi demonstrado é a viabilidade física do efeito de carga coletiva, que é a base de seu potencial.

Não se espera que essas baterias substituam os produtos químicos convencionais (lítio, sódio, etc.), mas sim, que tenham aplicações em nanodispositivos, sensores e tecnologias quânticas, onde a recarga ultrarrápida e a eficiência quântica podem fazer a diferença.



Identidade Quebrada: Um Chamado à Ação na Era da IA

Por Jordy Javier Ruiz Sánchez

Trabalho nas trincheiras da segurança digital há anos e testemunhei uma verdade inconveniente: a maneira como concebemos a identidade está fundamentalmente quebrada. Por décadas, nos apegamos à ideia do nome de usuário e da senha como se fossem um castelo inexpugnável. Hoje, esse castelo é feito de areia, e a maré da Inteligência Artificial (IA) está subindo a uma velocidade que nos obriga a agir.

A IA não é apenas uma nova ferramenta no arsenal tecnológico; é o agente de mudança que redefine as regras do jogo. Tornou-se uma dualidade com a qual precisamos aprender a conviver: por um lado, é a maior ameaça que o gerenciamento de identidades já enfrentou e, por outro, nossa defesa mais poderosa. Esta não é apenas mais uma análise técnica, mas um chamado à ação com base no guia da Cloud Security Alliance sobre Gerenciamento de Identidades em IA Agêntica e em nossa própria pesquisa. Portanto, é hora de parar de falar sobre "portas" e começar a falar sobre "confiança".

Quando "ser" e "fazer" não são mais suficientes

Em sua essência, o gerenciamento de identidades sempre buscou responder a duas perguntas simples: "Quem é você?" (autenticação) e “O que você tem permissão para fazer?" (autorização).

Costumo usar analogias simples para explicar isso: identidade é como entrar no prédio onde você trabalha. Você mostra seu crachá para o segurança, que verifica sua foto e nome na lista. Isso é autenticação. Uma vez lá dentro, seu cartão só dá acesso a um andar e a uma área, mas não a outros espaços, como o escritório do CEO ou outros departamentos. Isso é autorização. Este modelo nos serviu bem por um tempo; no entanto, a IA o tornou obsoleto. O desafio agora não é apenas verificar uma identidade estática, mas compreender um contexto dinâmico e responder a perguntas muito mais complexas: Sob qual cadeia de delegação este agente de IA está operando? Quais permissões ele precisa para esta tarefa específica (e apenas pelos próximos cinco minutos)? Como posso garantir, de forma criptográfica, que ele não foi falsificado?

O Paradoxo da IA: O Incendiário e o Bombeiro

Hoje, a IA coloca ferramentas extremamente poderosas tanto nas mãos de atacantes quanto de defensores. Do meu ponto de vista, trata-se de uma corrida tecnológica na qual não podemos nos dar ao luxo de ficar para trás.

A ameaça: A industrialização do engano

A IA generativa democratizou a fraude: de e-mails de *phishing* com erros ortográficos até mensagens personalizadas, produzidas com “engenharia de prompts”, quase impossíveis de diferenciar de comunicações legítimas. Por outro lado, os famosos *deepfakes* e identidades sintéticas. Processos que antes considerávamos garantidos, como a verificação do cliente (Conheça seu Cliente), tornaram-se um campo minado. O invasor não precisa mais roubar uma credencial; ele pode fabricar uma identidade biometricamente perfeita que engana nossos sistemas.

A defesa: em direção à confiança adaptativa

Felizmente, a própria IA nos oferece a solução. O velho sonho de "prevenir a violação" morreu. Devemos assumir que o invasor já está lá dentro e concentrar nossos esforços em detectá-lo e respondê-lo rapidamente. É aqui que nasce a Detecção e Resposta a Ameaças de Identidade (ITDR), uma disciplina que usa IA para aprender como se comportar com cada identidade (humana ou não) e detectar quaisquer anomalias em tempo real.

Imagine um desenvolvedor que trabalha sempre em Madri, das 9h às 17h. Se a conta dele tentar acessar repentinamente um repositório de código de um servidor no Leste Europeu às 3h da manhã, o sistema não o bloqueia cegamente. Em vez disso, ele ativa a autenticação adaptativa: ela requer um segundo fator infalsificável, como uma chave física FIDO2. Não se trata de construir muros mais altos, mas de ter um sistema imunológico inteligente.

A Nova Força de Trabalho: Governando Identidades Não Humanas

Se você me perguntar qual é o maior ponto cego na segurança hoje, minha resposta é clara: tratamos as máquinas como cidadãos de segunda classe.

Na maioria das empresas, o número de APIs, microsserviços, contêineres e agentes de IA já excede em muito o de colaboradores humanos. Eles são a nossa nova força de trabalho digital, e o maior erro estratégico é gerenciá-los com as ferramentas do passado.

Essas identidades não usam senhas. Elas operam com tokens, certificados e chaves de API. O desafio é gerenciar seu ciclo de vida na velocidade da máquina, não na velocidade humana. A prática de incorporar uma chave secreta no código de um aplicativo é, simplesmente, negligência. A solução é abandonar as credenciais estáticas e de longa duração em favor de credenciais efêmeras e de curta duração. Um aplicativo deve ser capaz de provar sua própria identidade para obter um token válido por apenas alguns minutos, para uma tarefa específica, e então desaparecer. Como a Cloud Security Alliance corretamente aponta, os protocolos tradicionais são insuficientes para a natureza dinâmica da IA. A fronteira agora está nos Identificadores Descentralizados (DIDs) e nas Credenciais Verificáveis (VCs), que permitem que um agente prove criptograficamente quem é, o que pode fazer e quem lhe deu essa autoridade. Estamos construindo uma economia de confiança para máquinas.

Um ciclo de vida para cada identidade: princípios para ação

Portanto, uma abordagem moderna ao IAM deve ser implacável em todas as etapas do ciclo de vida, tanto para humanos quanto para máquinas.

- Durante o provisionamento, o primeiro passo é um inventário. Atribua um proprietário humano a cada identidade não humana para eliminar "contas órfãs". Para seus colaboradores, exija MFA resistente a *phishing*, como *passkeys* (FIDO2), desde o primeiro dia. Por enquanto, esta é a medida mais eficaz que podemos tomar.

- Ao longo do seu ciclo de vida (gerenciamento – modificação – mudança), a governança deve ser contínua. Revisões periódicas de acesso, auxiliadas por IA que sugere a remoção de permissões não utilizadas (engenharia de funções), são cruciais para manter o princípio do menor privilégio.

- Durante o desprovisionamento: esta fase é crítica. Quando um colaborador deixa uma empresa ou um aplicativo é desativado, seus acessos devem ser revogados de forma instantânea e completa.

Credenciais órfãs são *backdoors* esperando para serem descobertas. Precisamos de sistemas que possam realizar uma revogação global e imediata de todas as sessões ativas para uma identidade comprometida.

Conclusão: Identidade é o Novo Perímetro

Deixamos para trás a era em que o gerenciamento de identidades era focado em uma função de suporte de TI. Hoje, é o núcleo estratégico que permite ou dificulta a inovação segura com IA. Não gerenciamos mais pessoas acessando sistemas; governamos um ecossistema vivo de humanos, máquinas e agentes autônomos. Adotar essas estratégias não é uma opção, é um imperativo.

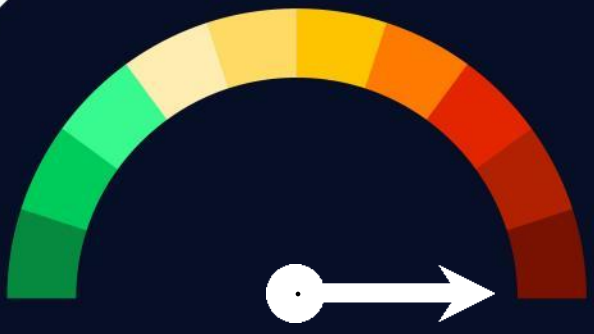
Em um mundo em que a identidade pode ser fabricada, nossa única defesa é uma confiança que nunca é assumida e sempre verificada. “Zero Trust” não é uma arquitetura; é a filosofia que nos permitirá navegar nesta nova fronteira. E a IA, com todos os seus riscos, é a opção mais viável que temos para fazer isso em escala.

Jordy Javier Ruiz Sánchez
Analista de Cibersegurança

Vulnerabilidades

Vulnerabilidade Crítica no SAP NetWeaver

Data: 8 de setembro de 2025
CVE: CVE-2025-42944



CVSS: 10

CRÍTICA

Descrição

A vulnerabilidade CVE-2025-42944 representa uma ameaça crítica a ambientes que executam o SAP NetWeaver, pois permite a execução remota de comandos sem a necessidade de autenticação.

Essa falha se baseia na desserialização insegura (CWE-502) devido ao módulo vulnerável RMI-P4, que atua como uma porta de entrada para um invasor manipular objetos serializados e executar código arbitrário no servidor.

A falta de autenticação prévia amplifica o risco de ataque, permitindo que agentes maliciosos externos interajam diretamente com o sistema vulnerável.

Solução

As recomendações da SAP são as seguintes:

- Atualização imediata para a versão mais recente disponível;
- Implementação de controles de acesso adicionais para a ferramenta.

Produtos afetados

Esta vulnerabilidade crítica afeta:

- SAP NetWeaver ServerCore versão 7.50

Referências

- nvd.nist.gov
- zeropath.com

Vulnerabilidades

Vulnerabilidade no WhatsApp explorada em iOS e MacOS

Data: 29 de agosto de 2025
CVE: CVE-2025-55177

CVSS: 5.4

MEDIA

Descrição

A vulnerabilidade de clique zero CVE-2025-55177 no WhatsApp afeta iOS, iPadOS e macOS.

Isso ocorre devido à autorização insuficiente durante a sincronização do dispositivo, permitindo a execução de código ou a instalação de *spyware* simplesmente pelo recebimento de uma mensagem criada.

A falha explora a maneira como o WhatsApp processa objetos e arquivos de mídia, causando corrupção de memória.

Embora tenha sido detectada em alguns casos, ela destaca o alto risco de ataques invisíveis e cadeias de exploração para espionagem.

Solução

Recomenda-se aplicar imediatamente os patches oficiais do WhatsApp e da Apple:

- iOS e iPadOS: versão 2.25.21.73 ou posterior;
- macOS: versão 2.25.21.78 ou posterior.

Produtos afetados

As versões vulneráveis são as seguintes:

- iOS: de 2.22.25.2 a 2.25.21.73
- macOS: até 2.25.21.78

Referências

- incibe.es
- nvd.nist.gov

TLP:WHITE

A Citrix corrige vulnerabilidades no NetScaler ADC e Gateway.

Data: 26 de agosto de 2025
CVE: CVE-2025-7775 e mais 2

Crítica

Descrição

Diversas vulnerabilidades do Citrix NetScaler foram descobertas recentemente.

A CVE-2025-7775 é uma vulnerabilidade crítica de estouro de buffer que pode permitir a execução remota de código ou causar uma negação de serviço. Isso se aplica ao NetScaler configurado como um gateway ou servidor virtual AAA, vinculado a serviços IPv6 ou a um servidor virtual CR do tipo HDX.

A CVE-2025-7776, de alta gravidade, também é um estouro de buffer que pode causar comportamento incorreto ou uma negação de serviço, exigindo que o NetScaler seja configurado como um gateway com um perfil PCoIP vinculado.

Enquanto isso, a CVE-2025-8424 é uma vulnerabilidade de controle de acesso impróprio na interface de gerenciamento, que pode permitir ações não autorizadas se o invasor tiver acesso ao NSIP, ao IP de gerenciamento do cluster, ao IP do site GSLB local ou ao SNIP com privilégios administrativos.

Produtos afetados

- NetScaler ADC e NetScaler Gateway: Versões anteriores à 13.1-59.22 e versões anteriores a 14.1-47.48;
- NetScaler ADC FIPS/NDcPP: Versões anteriores a 13.1-37.241 e 12.1-55.330, respectivamente.

Solução

O Cloud Software Group recomenda que os clientes afetados instalem as versões mais atualizadas.

Referências

- nvd.nist.gov
- support.citrix.com

Google corrige vulnerabilidade no Android Runtime

Data: 29 de agosto de 2025
CVE: CVE-2025-48543

Alta

Descrição

O Google corrigiu a vulnerabilidade de escalonamento de privilégios conhecida como CVE-2025-48543.

Esta vulnerabilidade explora uma vulnerabilidade de segurança após liberação no Android Runtime para escapar da *sandbox* do Chrome e comprometer o processo *system_server* em dispositivos Android.

Isso pode, posteriormente, levar ao escalonamento de privilégios locais sem exigir nenhuma interação do usuário.

A exploração bem-sucedida da CVE-2025-48543 pode permitir que invasores obtenham privilégios elevados no dispositivo Android.

Produtos afetados

Os produtos afetados incluem:

- Google Android 16;
- Google Android 15;
- Google Android 14;
- Google Android 13.

Solução

O Google reforçou a segurança do Android Runtime (ART), distribuindo o patch via Google Play para proteger imediatamente dispositivos habilitados para GMS, mesmo antes das atualizações do sistema operacional.

Referências

- nvd.nist.go
- fonte.android.com

Eventos

Cyber Security World Asia
8 - 9 de outubro

Este importante evento de cibersegurança ocorrerá nos dias 8 e 9 de outubro de 2025, no Marina Bay Sands Expo & Convention Centre, em Singapura. O encontro reunirá líderes e especialistas para debater temas como Zero Trust, inteligência artificial aplicada à defesa cibernética, gestão de identidades, segurança na nuvem, proteção de redes, criptografia quântica e resposta a incidentes, consolidando-se como o principal evento da região dentro da Tech Week Singapore.

Link

Fórum InCyber Canadá
14 – 15 de outubro

O fórum internacional sobre cibersegurança e confiança digital acontecerá nos dias 14 e 15 de outubro de 2025, no Palais des Congrès, em Montreal (Canadá). O evento abordará ameaças emergentes, *ransomware*, segurança na nuvem, inteligência artificial, criptografia quântica, proteção de infraestrutura crítica e mobilidade inteligente, tornando-se o principal ponto de encontro da América do Norte para líderes e especialistas do setor.

Link

InfoSec World 2025
27 - 29 de outubro

A conferência de cibersegurança ocorrerá de 27 a 29 de outubro de 2025, no Disney's Coronado Springs Resort, Flórida (EUA). O evento discutirá inteligência de ameaças, segurança na nuvem, gestão de identidades, Zero Trust, resiliência, resposta a incidentes e riscos na cadeia de suprimentos, firmando-se como fórum essencial para profissionais e líderes do setor.

Link

Recursos

➢ Índice de Cibersegurança da UE 2024

O Índice de Cibersegurança da UE, publicado pela ENISA, avalia a postura de cibersegurança dos Estados-Membros da UE, medindo áreas-chave como políticas, capacidades técnicas, mercado e indústria e operações. O relatório identifica pontos fortes e lacunas, destacando desafios na adoção de IA, certificação CSIRT, investimentos em cibersegurança e acesso a fundos de inovação, servindo como ferramenta de referência para aprimorar a resiliência digital e harmonizar estratégias em nível europeu.

Link

➢ Guia Técnico de Implementação da NIS2

A ENISA publica este guia para auxiliar entidades de infraestrutura digital, provedores de serviços de TIC e plataformas digitais na implementação da Diretiva NIS2. Ele oferece orientações práticas sobre gestão de riscos, políticas de segurança, tratamento de incidentes, continuidade de negócios, segurança da cadeia de suprimentos e desenvolvimento seguro, facilitando a adoção de medidas de cibersegurança e fortalecendo a resiliência digital em setores críticos.

Link

➢ Metodologia do Panorama de Ameaças Cibernéticas

A ENISA atualizou sua metodologia do Panorama de Ameaças Cibernéticas para oferecer uma abordagem mais prática e estruturada à produção de relatórios horizontais, temáticos e setoriais. A metodologia define processos-chave, partes interessadas, ferramentas e elementos de conteúdo, promovendo transparência e consistência na análise de ameaças cibernéticas na Europa.

Link

Assine a RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com