Número 119 | Outubro de 2026

NTT DATA

Radar

A revista de cibersegurança



Antecipar-se também é governar

Por Diego Javier Rocha Rodríguez

Durante anos, a gestão de riscos se apoiou em uma lógica conhecida: identificar, avaliar, estabelecer controles e revisar periodicamente. Esse modelo continua necessário, mas o ambiente em que as organizações operam hoje está mudando em um ritmo que também exige uma evolução na forma como conduzimos a governança.

A inteligência artificial talvez seja o exemplo mais evidente. Sua incorporação a processos, decisões, dados e sistemas está criando novas oportunidades de transformação, mas também modifica continuamente a exposição das organizações. O risco já não muda apenas quando ocorre um incidente ou surge uma nova regulamentação. Esse risco pode mudar com uma integração, um novo modelo, um fornecedor, uma decisão automatizada ou um nível diferente de autonomia.

Nesse cenário, adotar uma governança proativa significa reduzir a distância entre o momento em que o risco muda e aquele em que conseguimos identificá-lo e agir.

Isso exige a transição de análises pontuais e periódicas do risco para uma visão mais dinâmica. Conectar informações provenientes de ativos, dados, identidades, fornecedores, vulnerabilidades e incidentes; detectar sinais precoces; compreender dependências e usar esse contexto para priorizar decisões antes que uma exposição gere impacto.

Mas contar com mais informações e maior capacidade de antecipação traz outra questão fundamental: podemos confiar na inteligência que usamos para tomar decisões?

À medida que a IA deixa de apenas recomendar e passa a executar ações, a confiança deixa de ser uma declaração de princípios. Ela precisa ser projetada, supervisionada e comprovada.

Precisamos entender como uma decisão é tomada, verificar as informações que a sustentam, estabelecer limites claros e manter mecanismos que permitam questionar, corrigir ou reverter uma ação quando necessário.

Nesta edição da RADAR, dedicada a governança proativa e à gestão de riscos, abordamos essas duas vertentes de uma mesma evolução. Em “IA e risco corporativo: da avaliação periódica a um monitoramento contínuo”, exploramos como observar os riscos de forma mais contínua, correlacionar sinais e antecipar mudanças na exposição. Em “Intelligence we trust: a confiança como nova fronteira da IA”, concentramos a atenção nas condições necessárias para que essa inteligência seja compreensível, verificável, controlável e responsável.

Gerenciar riscos de forma proativa não significa prever tudo o que pode acontecer. Significa desenvolver a capacidade de enxergar antes, compreender melhor e decidir no momento certo. Porque, em um ambiente em que a tecnologia evolui continuamente, governar já não pode significar apenas revisar o que aconteceu. Também significa estar preparado para reconhecer o que está por vir.



Diego Javier Rocha Rodríguez
Cybersecurity Expert Engineer

 © Copyright NTT DATA, Inc.

As portas de Nanao: governar o risco antes que o castelo desmorone

Cibercrônica por Juan Pablo Campo Téllez

Uma organização não é segura simplesmente porque tem boas muralhas. Também precisa saber quem pode abrir as portas. A gestão de riscos não deveria começar quando ocorre um incidente, mas muito antes, quando ainda é possível identificar as condições que poderiam permitir que ele acontecesse.

Em 1576, Uesugi Kenshin, um dos senhores da guerra mais temidos do Japão feudal, liderou suas forças contra o castelo de Nanao, na província de Noto. Construído sobre o monte Sekidō e projetado para resistir a longos cercos, Nanao representava exatamente o que se esperava de uma fortaleza da época: manter o inimigo do lado de fora.

Kenshin tentou e fracassou. Quando retornou em 1577, iniciou um novo cerco que se prolongaria por meses. No entanto, a batalha mais importante já não acontecia diante das defesas, mas dentro delas. Uma epidemia enfraqueceu os defensores, as tensões políticas aumentaram e as disputas internas acabaram fragmentando a estrutura que sustentava a fortaleza.

Segundo os registros históricos compilados pela cidade de Nanao, em 15 de setembro de 1577, Yusa Tsugumitsu e seus aliados se rebelaram e, por fim, abriram os portões para as forças de Uesugi Kenshin. Depois de meses tentando entrar, o inimigo já não precisava conquistar as muralhas.

Nanao não desmoronou porque suas pedras eram frágeis demais. A fortaleza ruiu quando as condições que garantiam sua segurança deixaram de ser governadas.

Mais de quatro séculos depois, as organizações continuam construindo castelos. As muralhas agora são firewalls; os postos de vigilância, centros de operações de segurança; os fossos, mecanismos de segmentação; e as portas são protegidas por MFA, sistemas de gestão de identidades, SIEM, EDR e plataformas de monitoramento.

As empresas investem milhões no fortalecimento dessas defesas, mas uma organização não é segura simplesmente porque tem boas muralhas. Também precisa saber quem pode abrir as portas.

Esse é um dos princípios fundamentais da gestão proativa de riscos. A gestão de riscos não deveria começar quando ocorre um incidente, mas muito antes, quando ainda é possível identificar as condições que poderiam permitir que ele acontecesse.

Uma conta administrativa que mantém privilégios desnecessários, um fornecedor com acesso permanente a um ambiente crítico, uma exceção temporária de segurança que nunca mais é revisada ou um sistema legado que continua em operação podem parecer, isoladamente, decisões justificáveis. No entanto, quando essas decisões se acumulam e deixam de ser supervisionadas, podem se transformar nas portas de Nanao.

O problema é que o risco não permanece estático. À medida que a organização evolui, surgem novos fornecedores, aplicações, vulnerabilidades e identidades; funções, arquiteturas e permissões sofrem alterações. Uma decisão aceitável meses atrás pode posteriormente se transformar em uma exposição crítica. Por isso, governar o risco exige revisar continuamente as condições capazes de modificá-lo.

Um exemplo mostra até onde esse problema pode chegar. Em fevereiro de 2024, a Change Healthcare, uma das principais plataformas de processamento de transações do sistema de saúde dos Estados Unidos, sofreu um ciberataque que causou grandes interrupções em serviços relacionados a prescrições, solicitações de reembolso médico e pagamentos.

Os atacantes usaram credenciais comprometidas para acessar remotamente um portal Citrix que não tinha autenticação multifator habilitada. Depois de entrar, conseguiram se movimentar lateralmente pelo ambiente, extrair informações e, posteriormente, implantar ransomware.

O caso é particularmente relevante porque o ponto de entrada não foi uma vulnerabilidade desconhecida e sofisticada. A porta existia, era usada legitimamente para acesso remoto e simplesmente não contava com uma proteção que hoje é considerada fundamental.

É justamente aí que surge a diferença entre gerenciar vulnerabilidades e governar o risco. Não se trata apenas de perguntar quais vulnerabilidades existem, mas quais decisões, exceções e condições estão gerando uma exposição futura.

Por que um sistema crítico continua sem MFA? Quem aceitou esse risco? Por quanto tempo essa aceitação deveria permanecer válida? Que mecanismo deveria verificar se essa condição foi corrigida?

A gestão proativa de riscos transforma essas perguntas em um processo contínuo e exige que a organização reveja suas decisões à medida que os negócios evoluem.

ssa perspectiva ganhou ainda mais relevância quando, em fevereiro de 2024, o NIST publicou a versão 2.0 de seu Cybersecurity Framework e incorporou GOVERN como uma sexta função, ao lado de Proteger, Detectar, Responder e Recuperar.

Com isso, o NIST explicitou que a gestão da cibersegurança também exige estabelecer estratégias de risco, responsabilidades, políticas, mecanismos de supervisão e gestão dos riscos associados a terceiros e às cadeias de suprimentos. Assim, a cibersegurança deixa de ser responsabilidade exclusiva de quem administra ferramentas técnicas e passa a fazer parte da gestão de riscos empresariais e das decisões da liderança.

Um firewall pode bloquear uma conexão, mas não pode decidir quanto risco uma organização está disposta a aceitar. Um EDR pode identificar uma atividade suspeita, mas não pode determinar quem deve assumir a responsabilidade por um sistema crítico.

Uma solução de IAM pode restringir permissões, mas não pode decidir por que um fornecedor precisa de determinado nível de acesso nem por quanto tempo deve mantê-lo.

Essas são decisões de governança. Em outras palavras, alguém precisa saber onde estão as portas, quem tem as chaves e em quais circunstâncias pode usá-las.

Gerenciar riscos de forma proativa significa evitar que decisões se acumulem silenciosamente. Exige a identificação dos responsáveis reais pelos riscos, prazos para as exceções, revisões periódicas dos acessos privilegiados, acompanhamento de terceiros e mecanismos que permitam detectar quando a exposição da organização foi alterada.

Também exige uma cultura em que identificar um risco não seja interpretado como fracasso. Uma governança madura não busca organizações em que ninguém encontra problemas. Uma boa governança busca organizações capazes de encontrá-los antes dos adversários.

Durante meses, os defensores de Nanao puderam observar o exército inimigo do outro lado das fortificações. Sabiam onde estava a ameaça e haviam construído defesas capazes de mantê-la à distância. O que não conseguiram controlar foi a deterioração que ocorria atrás das próprias muralhas.

Esse continua sendo um dos grandes desafios da governança moderna.

Uma organização verdadeiramente resiliente não é aquela que confia que suas muralhas são impenetráveis, mas aquela que avalia continuamente o que poderia enfraquecê-las, quem pode abrir suas portas e quais decisões poderiam transformar uma fortaleza em uma falsa sensação de segurança.

Porque a gestão eficaz de riscos não começa quando o exército aparece diante do castelo. Começa muito antes, quando ainda há tempo para decidir quem fica com as chaves.



Juan Pablo Campo Téllez
Cybersecurity Engineer

IA e risco corporativo: da avaliação periódica a um monitoramento contínuo

Artigo por Ángel Fernando Andrango Mejía

A inteligência artificial evolui mais rápido do que as organizações conseguem antecipar seus riscos. Nesse cenário, a vantagem competitiva já não estará apenas na adoção da IA, mas no desenvolvimento de capacidades para identificar, compreender e governar seus riscos de forma contínua.

Quando a velocidade da IA supera o ritmo da gestão de riscos

As matrizes de risco continuam sendo ferramentas valiosas para priorizar e apoiar a tomada de decisões. No entanto, quando a IA altera rapidamente o nível de exposição de uma organização, essas ferramentas precisam ser alimentadas com informações atualizadas sobre as tecnologias utilizadas, os dados processados, os acessos concedidos, as integrações habilitadas, as vulnerabilidades detectadas, os incidentes e as dependências operacionais.

O objetivo não é substituir a matriz de riscos, mas complementá-la com uma capacidade de observação contínua que permita compreender como a exposição da organização está mudando e apoiar decisões mais oportunas.

Dessa forma, a gestão de riscos evolui de análises pontuais para uma visão mais dinâmica, capaz de identificar mudanças e antecipar cenários antes que gerem impactos relevantes para os negócios.

A nova geração de modelos: o que muda?

A atenção do mercado costuma se concentrar em cada novo modelo de IA que surge. No entanto, o verdadeiro desafio não está em uma tecnologia específica, mas em uma tendência mais profunda: a capacidade dessas soluções de ampliar continuamente o que pessoas e organizações podem fazer.

A IA não introduz apenas novas formas de exposição. Também altera a velocidade, a escala e a interdependência dos riscos existentes. Uma mesma solução pode processar informações sensíveis, conectar-se a sistemas críticos, automatizar decisões e, ao mesmo tempo, depender de fornecedores externos.

Essas capacidades oferecem importantes oportunidades de produtividade e transformação, mas também podem ampliar a exposição na mesma velocidade em que a tecnologia é adotada.

O risco surge quando essas capacidades operam sem visibilidade, supervisão ou governança suficientes. Por isso, é fundamental compreender onde podem se materializar as principais exposições e como podem afetar a organização.

Riscos estratégicos para uma gestão empresarial proativa

A IA aumenta a complexidade do risco porque reúne dados, sistemas, decisões automatizadas e dependências externas em uma única solução.

Por isso, uma gestão proativa deve observar pelo menos cinco dimensões:

Dados e privacidade

Uso indevido de informações sensíveis, novos fluxos de dados e acessos não previstos.

Cibersegurança

Falsificação de identidade, exploração de vulnerabilidades e integrações com modelos e agentes.

Operações

Dependências tecnológicas, falhas, mudanças de fornecedores e adoção de IA em processos críticos.

Conformidade e ética

Falta de rastreabilidade, responsáveis definidos ou critérios regulatórios claros.

Reputação e negócios

Erros ou incidentes com impacto sobre clientes, confiança, decisões ou marca.

A IA, portanto, não constitui uma categoria isolada de risco. Seu impacto atravessa simultaneamente a cibersegurança, a privacidade, a continuidade operacional, a conformidade e a reputação.

 © Copyright NTT DATA, Inc.

De um registro de riscos a um radar inteligente

A principal diferença entre uma matriz tradicional e um radar inteligente está na capacidade de acompanhar a evolução do risco.

Matriz de riscos
Identifica → Avalia → Registra → Revisa

Radar inteligente
Descobre → Correlaciona → Prioriza → Responde → Aprende

As duas abordagens são complementares. Enquanto a matriz permite estruturar e avaliar riscos conhecidos, o radar incorpora uma lógica de observação contínua que conecta sinais provenientes de diferentes fontes para compreender como a exposição está mudando.

Essa abordagem permite:

1. Descobrir ferramentas, modelos, agentes e integrações.
2. Correlacionar sinais provenientes de dados, usuários, sistemas e fornecedores.
3. Priorizar os riscos de maior impacto e criticidade.
4. Responder por meio de controles e ações de mitigação.
5. Aprender com incidentes e novos padrões para aprimorar continuamente a capacidade de monitoramento.

Resumindo, a matriz mostra onde está o risco; o radar ajuda a compreender para onde esse risco está se dirigindo.

Indicadores que antecipam o risco

Uma capacidade de observação contínua precisa de indicadores que permitam identificar sinais precoces antes que se transformem em incidentes ou gerem impactos relevantes para os negócios.

Entre os indicadores que podem ser especialmente úteis estão:

- Ferramentas de IA sem governança definida.
- Casos de uso de IA sem um responsável de negócio designado.
- Integrações de IA conectadas a sistemas críticos.
- Vulnerabilidades associadas a modelos, fornecedores ou conectores.
- Tempos de detecção e resposta a eventos relacionados à IA.

O monitoramento contínuo desses sinais ajuda a identificar tendências emergentes e a evoluir de uma gestão predominantemente reativa para uma capacidade preventiva e orientada à antecipação.

Inovar com velocidade, governar com antecipação

Nos próximos anos, o fator de diferenciação não será apenas quem adota mais inteligência artificial, mas quem consegue compreendê-la, supervisioná-la e governá-la melhor.

As organizações que desenvolverem capacidades de observação contínua estarão mais preparadas para aproveitar os benefícios da IA e, ao mesmo tempo, gerenciar de forma proativa seus impactos sobre a informação, a segurança, as operações e a confiança.

Porque, em um ambiente em que os modelos evoluem constantemente, o risco já não pode ser gerenciado olhando apenas para o passado. É preciso gerenciá-lo de olho no horizonte.



Ángel Fernando Andrango Mejía
Cybersecurity Lead Analyst

Intelligence we trust: a confiança como nova fronteira da IA

Artigo por María Pilar Torres Bruna

A inteligência artificial já é capaz de nos surpreender. O próximo desafio é mais profundo: garantir que suas decisões sejam compreensíveis, verificáveis e seguras à medida que ganha autonomia.

Hoje, a Inteligência Artificial já redige, analisa, prevê, recomenda, automatiza processos e apoia decisões que antes dependiam exclusivamente das pessoas. Sua capacidade é extraordinária, mas a IA já deixou para trás a etapa em que precisava provar seu potencial. Estamos entrando em uma nova fase de adoção dessa tecnologia, em que a questão passa a ser: em quais processos ou decisões podemos confiar nela?

À medida que passamos a depender da IA para responder a consultas complexas e até executar ações — por exemplo, priorizar um alerta, aprovar uma operação, interagir com um cliente ou recomendar uma decisão crítica —, a confiança se torna uma condição essencial para aprofundar seu uso e avançar com segurança em sua adoção. A IA já nos ajuda a criar sistemas mais capazes e sofisticados. Agora, o foco está em torná-los confiáveis.

Isso muda a conversa e também a arquitetura que sustenta a IA dentro de uma organização. A confiança é muito mais do que uma declaração de princípios ou uma política de segurança. É preciso que se traduza em uma capacidade operacional, que as organizações possam projetar, implementar, monitorar e demonstrar.

Do fascínio à confiança

Nos últimos anos, já exploramos o que a IA pode criar, quanto pode ajudar uma organização a acelerar seus negócios e quais tarefas pode transformar.

No entanto, à medida que a tecnologia começa a operar com maior autonomia, precisamos entender como chegou a uma conclusão, com quais informações trabalhou, quais são seus limites e quem pode intervir caso algo não funcione como deveria. Precisamos de transparência e rastreabilidade nos processos dessa tecnologia.

A IA pode gerar inteligência; os agentes podem transformar essa inteligência em ação. Entretanto, é a confiança que torna essa ação aceitável, segura e escalável.

Uma organização pode incorporar IA a diversos processos, mas precisa ser capaz de explicar, controlar e auditar suas decisões. Sem essa capacidade, será difícil ampliar o uso da IA e transmitir confiança aos colaboradores e clientes da organização. É a confiança que permite passar de uma prova de conceito atraente para uma adoção efetiva.

Três perguntas para construir confiança

Uma forma simples de abordar esse desafio é partir de três perguntas fundamentais.

1. Podemos entendê-la?

Se um sistema recomenda uma ação, as pessoas responsáveis precisam ser capazes de compreender, pelo menos no nível adequado ao contexto, por que ele fez essa recomendação.

A transparência e a rastreabilidade permitem explicar, com base nas informações fornecidas, os resultados apresentados, compreender a recomendação e explicá-la quando necessário.

Isso é especialmente relevante em decisões de alto impacto, que afetam a vida das pessoas, como sua trajetória profissional, ou que podem até salvar uma vida. Se um sistema de IA sugerir o bloqueio de uma transação, a rejeição de um candidato, a priorização de um caso médico ou a alocação de um recurso, a decisão deve ser explicável.

2. Podemos verificá-la?

A qualidade de uma resposta de IA é proporcional à qualidade das informações que a alimentam. Os dados precisam estar completos e atualizados, e é necessário garantir que não tenham sido manipulados.

A confiança começa na origem dos dados. As organizações precisam saber de onde vêm as informações, quem as modifica, quando foram alteradas e se sofreram qualquer outra modificação.

O processo de alteração dos dados precisa ser rastreável, já que a rastreabilidade se torna cada vez mais relevante em um ambiente no qual circulam conteúdos sintéticos, dados provenientes de múltiplas fontes e decisões automatizadas.

Verificar também significa validar a autenticidade do conteúdo e das identidades envolvidas. A fonte — seja uma organização, uma pessoa ou até mesmo um agente — precisa ser confiável.

Na era da IA, conhecer a origem e a integridade das informações deixa de ser apenas um requisito técnico e se torna uma condição para a confiança.

3. Podemos questioná-la?

A última dimensão da confiança envolve os mecanismos disponíveis para supervisionar, contestar, corrigir ou reverter as decisões tomadas pela IA quando o contexto exigir.

Uma IA confiável e os agentes baseados em IA precisam ter limites claros. Devem saber o que podem fazer, a quais informações podem acessar e quando uma decisão precisa ser escalada para uma pessoa. Também deve ser possível intervir quando for detectado um comportamento inesperado, um desvio em relação às regras estabelecidas ou um sinal de manipulação.

Nesse ponto, a colaboração entre IA e cibersegurança assume uma nova dimensão.

A abordagem Zero Trust, tradicionalmente aplicada a usuários, dispositivos e conexões, também é relevante e útil para sistemas inteligentes. A regra é simples: confiança zero. Cada agente, modelo ou componente deve operar com permissões definidas, apenas com o nível mínimo de acesso necessário e sob validação contínua.

Segurança ativa para sistemas em evolução

Os riscos associados à IA vão além da infraestrutura e dos dados. Os modelos usados na tomada de decisões representam uma nova superfície de ataque. Um atacante pode tentar manipular as fontes de informação, alterar as permissões de um agente ou influenciar o comportamento de um modelo. Por isso, a segurança precisa evoluir de reativa para ativa e preditiva.

A ciberdefesa ativa e a segurança preditiva permitem detectar padrões, correlacionar grandes volumes de alertas e responder a determinadas ameaças com maior rapidez.

Uma autonomia madura é uma autonomia supervisionada: capaz de agir, mas também responsável por suas ações.

Governar a IA é governar suas decisões

Quando um sistema inteligente participa de processos relevantes, a governança não pode ser incorporada apenas no final. Precisa estar integrada desde o início.

Isso significa definir responsáveis, direitos de decisão, fluxos de escalonamento e critérios claros para intervenção. Também exige a geração de evidências, registros que permitam analisar o que aconteceu, quais dados foram utilizados, quais regras foram aplicadas e por que o sistema tomou determinada ação.

As trilhas de auditoria explicáveis são fundamentais para transformar a IA em uma capacidade supervisionada. Elas ajudam a responder a erros e permitem aprender com eles, aprimorar controles e fortalecer a confiança de clientes, colaboradores, órgãos reguladores e parceiros.

Confiança não é o que uma organização diz sobre sua IA. É aquilo que consegue comprovar, monitorar e governar.

A dimensão humana da confiança

Por fim, existe uma dimensão que nenhuma tecnologia pode resolver sozinha: a humana.

As pessoas não avaliam a confiança apenas com base em métricas de precisão. Também consideram se o sistema é justo, se respeita a privacidade, se responde em prazos razoáveis e se preserva espaços para a decisão humana, sobretudo em decisões sensíveis.

Para as pessoas, o que é aceitável em determinado contexto pode não ser em outro. As expectativas mudam de acordo com a cultura, o setor, o tipo de decisão e o impacto que essa decisão tem sobre as pessoas.

Construir confiança em IA exige escuta. Isso significa compreender como os usuários percebem os riscos, qual nível de autonomia estão dispostos a aceitar e em quais condições consideram legítima a participação de uma máquina em uma decisão que os afeta.

Tornar a confiança operacional



María Pilar Torres Bruna
Head of Cybersecurity IBIOL

Transformar a confiança em uma capacidade operacional significa avançar simultaneamente em três frentes:

Tornar a IA compreensível: explicar decisões e verificar conteúdo, fontes e procedência dos dados.

Tornar a IA controlável: estabelecer limites, gerenciar permissões, supervisionar agentes e detectar manipulações ou desvios.

Tornar a IA responsável: criar evidências, rastreabilidade e mecanismos de auditoria que permitam intervir e corrigir.

A inteligência artificial continuará avançando. Será mais poderosa, mais integrada e mais autônoma. Mas seu verdadeiro valor dependerá da confiança que for capaz de gerar.

Porque, na próxima etapa da IA, deixaremos de perguntar “Será que ela consegue fazer isso?” e passaremos a perguntar “Podemos confiar no que ela faz?”

Vulnerabilidades

Vulnerabilidade crítica no Cisco Nexus 9000 – execução remota de código

Data: 2 de setembro de 2026



CVSS: 9.8

CRÍTICA

Descrição

A Cisco publicou informações sobre uma vulnerabilidade que afeta determinados switches da série Nexus 9000 equipados com tecnologia Silicon One, com pontuação CVSS 3.1 de 9,8.

Um atacante remoto e não autenticado poderia explorar a vulnerabilidade para executar código com privilégios de root nesses dispositivos. O problema está relacionado à exposição das portas TCP 43210 e 43211 na VRF de camada 3 utilizada por padrão.

Esses equipamentos de rede são normalmente utilizados em infraestruturas críticas de data centers, onde uma exploração pode causar impactos significativos. Por esse motivo, é necessário realizar uma revisão prioritária dos dispositivos afetados.

Solução

A Cisco recomenda as seguintes medidas:

- Utilizar listas de controle de acesso à infraestrutura (iACL) para permitir apenas o tráfego necessário no dispositivo afetado.
- Implementar o patch para o Cisco NX-OS Software:
  - Live Protect Shield Software - 10.6(3)

Produtos afetados

Os seguintes identificadores do Cisco Nexus 9000 foram afetados:

- N9324C-SE1U y N9348Y2C6D-SE1U
- N9364E-SG2-O/Q
- N9396T12C-SE1 e N9348Y12C-SE1
- N9336C-SE1
- N9K-C9804 e N9K-C9808

Referências

- nvd.nist.gov
- rapid7.com

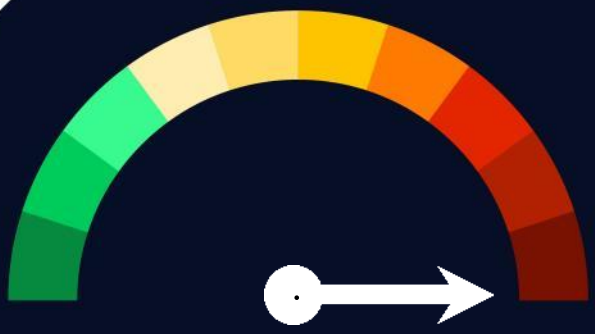
 © Copyright NTT DATA, Inc.

TLP:WHITE

Vulnerabilidades

Vulnerabilidades críticas no SonicWall SMA1000 com exploração ativa

Data: 1º de setembro de 2026
CVE: CVE-2026-83548 e mais 1



CVSS: 10

CRÍTICA

Descrição

A SonicWall publicou informações sobre duas vulnerabilidades que afetam os dispositivos SonicWall SMA1000:

- **CVE-2026-83548:** vulnerabilidade SSRF de pré-autenticação que permite que um atacante remoto não autenticado envie solicitações a recursos internos.
- **CVE-2026-83549:** vulnerabilidade de injeção de comandos no sistema operacional após a autenticação, que permite que um atacante com privilégios administrativos execute comandos arbitrários no sistema operacional do dispositivo.

Segundo confirmação da equipe de resposta a incidentes da SonicWall, as duas vulnerabilidades vêm sendo exploradas ativamente.
.

Solução

O fabricante recomenda que todas as organizações com dispositivos afetados adotem as seguintes medidas:

- Atualizar para a versão mais recente disponível na página oficial.
- Verificar os sistemas em busca de indicadores de comprometimento com o suporte da assistência técnica da SonicWall.
- Caso sejam identificados IoCs em algum dos sistemas, as ações recomendadas são:
  - Reinstalar o sistema operacional ou os dispositivos virtuais.
  - Redefinir todas as senhas de usuários e administradores.
  - Redefinir os tokens TOTP.

Produtos afetados

Os produtos afetados pelas duas vulnerabilidades são os modelos **6210, 7210 e 8200v** da série SonicWall SMA1000, nas seguintes versões:

- **12.4.3-03453** e anteriores
- **12.5.0-02835** e anteriores

Referências

- sonicwall.com
- rapid7.com
- securityweek.com

 © Copyright NTT DATA, Inc.

TLP:WHITE

Patch de segurança da Microsoft para vulnerabilidades críticas no SQL Server 2022

Data: 8 de setembro de 2026
CVE: CVE-2026-67378 e outras

Alta

Descrição

A Microsoft publicou novas atualizações de segurança destinadas a corrigir vulnerabilidades que afetam instalações tanto do Windows quanto do Linux. Dentro da linha GDR.

Esses patches corrigem diferentes tipos de vulnerabilidade, como execução remota de código, elevação de privilégios, divulgação de informações, negação de serviço e evasão de recursos de segurança.

Entre as vulnerabilidades de maior destaque estão a CVE-2026-67378, uma vulnerabilidade de execução remota de código com CVSS 8,5, além das CVE-2026-67380, CVE-2026-67384 e CVE-2026-67385, que atingem uma pontuação CVSS de 8,8.

Produtos afetados

Os produtos afetados são:

- SQL Server 2022 RTM GDR.

Solução

Instalar os seguintes patches de segurança:

- KB5122771
- KB5122768

Referências

- support.microsoft.com
- catalog.update.microsoft.com

 © Copyright NTT DATA, Inc.

Patch de segurança do Adobe Commerce

Data: 7 de setembro de 2026
CVE: CVE-2026-75650

Crítica

Descrição

A Adobe publicou um patch de segurança urgente para corrigir uma vulnerabilidade crítica (CVSS 10,0) que afeta o Adobe Commerce/Magento e vem sendo explorada ativamente em ataques reais.

A vulnerabilidade CVE-2026-75650, também denominada StyleSmuggler, afeta o sistema de templates do Adobe Commerce/Magento e permite que um atacante remoto e não autenticado envie uma requisição especialmente manipulada para executar código PHP no servidor.

Em ataques recentes, observou-se a exploração dessa falha para implantar um backdoor desenvolvido em Rust e instalar uma PHP web shell no diretório de imagens do Magento.

Produtos afetados

Os produtos afetados por essa vulnerabilidade crítica são:

- Adobe Commerce versões 2.4.4-2026-aug a 2.4.9-2026-aug, bem como versões anteriores dentro dessas linhas.
- Adobe Commerce B2B versões 1.3.3-2026-aug, 1.3.4-2026-aug, 1.4.2-2026-aug, 1.5.2-2026-aug e 1.5.3-2026-aug, bem como versões anteriores.
- Magento Open Source versões 2.4.6-2026-aug a 2.4.9-2026-aug, bem como versões anteriores.

.

Solução

O fabricante recomenda aplicar imediatamente o patch **VULN-39341** e fazer a rotação das chaves de criptografia e das credenciais potencialmente expostas, incluindo credenciais de administrador, servidor, banco de dados, APIs e integrações.
Além disso, recomenda-se verificar os **IoCs** identificados nos ataques observados.

Referências

- helpx.adobe.com
- experienceleague.adobe.com
- sansec.io
- thehackernews.com

 | © Copyright NTT DATA, Inc.

TLP:WHITE

Eventos

ISACA 2026 Europe Conference
7 a 9 de outubro

A ISACA Europe Conference reunirá em Munique e em formato virtual profissionais e líderes de tecnologia, cibersegurança, auditoria, governança e gestão de riscos. Por seu foco em governança, riscos e tomada de decisões, o evento é especialmente relevante para organizações que buscam se antecipar a um ambiente tecnológico cada vez mais dinâmico.

Link

Cyber Security & Cloud Expo Europe 2026
19 a 20 de outubro

A Cyber Security & Cloud Expo Europe reunirá em Amsterdã profissionais responsáveis por cibersegurança, tecnologia e transformação digital. A agenda inclui liderança em cibersegurança e riscos empresariais, segurança em cloud, inteligência artificial, identidade, Zero Trust e conformidade.

Link

Congresso de Segurança da ISC2 2026
24 a 28 de outubro

O ISC2 Security Congress reunirá em Denver e em formato virtual profissionais da comunidade global de cibersegurança. A edição de 2026 inclui sessões sobre liderança, gestão de riscos, segurança da inteligência artificial e desafios de supervisão diante da inovação.

Link

Recursos

- **As novas regras da confiança: governança, risco e conformidade na era da IA**

Publicação da NTT DATA que analisa como a inteligência artificial, cloud, os ecossistemas digitais e a evolução da regulamentação estão transformando os modelos tradicionais de governança, riscos e conformidade. O conteúdo apresenta a evolução para uma abordagem de GRC mais integrada e proativa.

Link

- **Global Cybersecurity Outlook 2026**

Guia do NIST publicado em março de 2026, conecta a gestão de riscos cibernéticos aos riscos corporativos e às capacidades necessárias para responder a um ambiente tecnológico em constante evolução.

Link

- **NIST CSF 2.0: Guia rápido de segurança cibernética, gestão de riscos corporativos e gestão da força de trabalho**

Relatório do Fórum Econômico Mundial (WEF), em colaboração com a Accenture, que analisa os principais fatores que estão transformando o cenário global de cibersegurança: inteligência artificial, fragmentação geopolítica, cadeias de suprimentos e lacunas de competências.

Link

NTT DATA

CLIQUE AQUI E SIGA A RADAR

Powered by the cibersegurança NTT DATA team

br.nttdata.com