Fique um passo à frente: receba o Radar todo dia útil, de graça. **Inscreva-se → hubterritory.com/radar/inscricao**

UMA PUBLICAÇÃO HUB TERRITORY · INTELIGÊNCIA DE AMEAÇAS EDIÇÃO Nº 10

Radar de Ciberataques

Incidentes no Brasil, o resumo do mundo e as falhas que estão sendo exploradas

Quarta-feira, 25 de novembro de 2026 Janela: ter 24/11, 07h05 a qua 25/11, 06h57 Edição nº 10

0	0	3
CASOS NO BRASIL	CONFIRMADOS	FALHAS EXPLORADAS

MUNDO · SEGURANÇA DE FIREWALL

Campanha mira servidores de gerência Check Point; correção já está disponível

A GreyNoise relata ao menos 22 organizações como alvo desde outubro, entre elas de governo e energia, por meio de uma falha já corrigida (CVE-2026-16232). A recomendação é aplicar a correção e manter a gerência fora da internet. No Brasil, não houve novo incidente confirmado na janela.

Como ler: CONFIRMADO a vítima ou uma autoridade confirmou · EM ANDAMENTO caso ainda aberto · "Nota oficial" marca a fonte publicada pelo próprio afetado ou por autoridade.

Nenhum incidente novo no Brasil na janela.

NÃO FOI ATAQUE · GOVERNO ESTADUAL

Mato Grosso descarta ataque após instabilidade no sistema de ponto

O Sigpass, sistema de ponto dos servidores estaduais de Mato Grosso, ficou indisponível na manhã de 23/11. Em nota, a Seplag informou que a causa foi uma falha pontual de conectividade de rede, sem ataque nem comprometimento de dados, e liberou o trabalho remoto no período.

Lição para outros órgãos: conectividade redundante e um plano de contingência simples para sistemas internos ajudam a manter o serviço e a separar rapidamente uma falha técnica de um incidente de segurança.

Fonte: Gazeta Digital (com nota da Seplag-MT), 23/11

CORRIJA TAMBÉM · SEM ATAQUES RELATADOS

VMware vCenter e WHMCS ganham correções para falhas críticas

VMware (VMSA-2026-0011, 24/11): a Broadcom corrigiu 23 falhas, entre elas um novo bypass de autenticação no vCenter (CVE-2026-123903, CVSS 9,8). Não há exploração relatada, mas uma falha parecida no mesmo componente (CVE-2026-123890) já foi explorada. Atualizar o vCenter (8.0 U3m, 9.0.2.0300 ou 9.1.2) e manter o acesso restrito à rede de gestão.

WHMCS (23/11): a plataforma de gestão e cobrança usada por provedores e empresas de hospedagem corrigiu uma injeção de SQL que permite ler o banco sem login (CVE-2026-82981) e outras duas falhas. Não há ataques relatados; atualizar o WHMCS self-hosted para 9.1.2 ou 9.0.10.

Fontes: Nota oficial: Broadcom — VMSA-2026-0011, 24/11 · Nota oficial: WHMCS — boletim CVE-2026-82981, 23/11

Atualizações

CASOS DE EDIÇÕES ANTERIORES QUE MUDARAM

Idunno.AntiCsrf (ASP.NET WebForms): a CISA incluiu a CVE-2026-131914 no catálogo KEV em 24/11, com prazo até 27/11 para órgãos federais dos EUA. Segue sem correção: a saída é remover a biblioteca e trocar por proteção anti-CSRF nativa.

Fonte: Nota oficial: CISA — catálogo KEV (cópia oficial no GitHub), 24/11

MONAI Label (imagens médicas): a CVE-2026-133968 entrou no KEV em 23/11, com prazo até 26/11. Ainda não há pacote corrigido no PyPI; a correção está só no código-fonte.

Fonte: Nota oficial: CISA — catálogo KEV (cópia oficial no GitHub), 23/11

Equinor (Noruega): a autoridade norueguesa NSM ligou o ataque à falha explorada no Azure API Management (veja o Alerta); a Microsoft fechou o acesso em 19/11. Segundo a empresa, a produção segue normal.

Fonte: Nota oficial: NSM (Noruega) — medidas contra vulnerabilidade no Azure API Management, 23/11

Mundo

OS CASOS MAIS RELEVANTES DO PERÍODO

MUNDO · GERÊNCIA DE FIREWALL

Campanha com uso de IA mira servidores de gerência Check Point

A GreyNoise relata que um ator chamado GT13 combina agentes de IA e operação manual para explorar falhas em servidores Check Point Security Management desde o início de outubro. Ao menos 22 organizações de energia, engenharia, finanças, governo, indústria, mineração e transporte foram alvo, e a empresa contou 24 servidores de gerência comprometidos.

A principal falha usada, no SmartConsole (CVE-2026-16232), já tem correção e está no catálogo de falhas exploradas da CISA desde julho; também houve tentativas contra NetScaler, Ivanti, NetLogon, Exchange e vCenter. Prevenção: confirmar a correção, manter a gerência fora da internet e revisar os acessos administrativos recentes.

Fontes: SecurityWeek (relatório da GreyNoise), 24/11 · Cybersecurity Dive, 24/11 · Nota oficial: CISA KEV (CVE-2026-16232), 22/07

EUA · GOVERNO ESTADUAL

Colorado confirma ataque ao app de serviços do estado

O myColorado, app usado pelos moradores para identidade digital, documentos e serviços do estado, foi desligado depois que um ataque foi descoberto na noite de 18/11; em 24/11 seguia fora do ar. O escritório de TI do governo (OIT) diz que dados ligados a cerca de 150 mil dos 2,1 milhões de usuários provavelmente foram levados, sem detalhar quais.

Os serviços continuam pelos sites de cada órgão. Lição para outros governos: apps de serviço ao cidadão concentram dados e pedem monitoramento contínuo, testes de segurança periódicos e um canal alternativo de atendimento pronto para uso.

Fonte: The Record (declaração do OIT do Colorado), 24/11

EUA · INTELIGÊNCIA

Rede não classificada usada pela CIA e pelo ODNI é invadida

Uma rede não classificada compartilhada, usada pela CIA e pelo ODNI para análise de fontes abertas, foi invadida e teve informação não classificada exposta, segundo o New York Times (24/11). A agência geoespacial NGA também teria sido afetada.

O ODNI disse à CNN que sistemas classificados e capacidades críticas não foram atingidos; escopo, método e autoria não foram divulgados. Lição: redes auxiliares e de pesquisa também precisam de MFA, monitoramento e separação das redes principais.

Fontes: Federal News Network (AP), 24/11 · The Washington Post (AP), 24/11 · Cyber Security News (cita CNN e Washington Examiner), 25/11

LITUÂNIA · ADUANA

Alfândega da Lituânia confirma invasão e retoma serviços aos poucos

A alfândega lituana detectou um ataque em 10/11 e desligou o BAP, portal de acesso a serviços aduaneiros e a alguns sistemas da Comissão Europeia, o que afetou plataformas da UE como o ICS2. Desde 16/11 parte dos serviços funciona pelo portal de governo eletrônico.

O órgão confirmou acesso não autorizado e possível exposição de dados de algumas centenas de usuários que acessaram o portal em 9 e 10/11; segundo a direção, os invasores tentaram chegar a outros sistemas do governo. Lição para portos e aduanas: segmentar os portais de acesso externo e exigir MFA reduz o alcance de uma invasão.

Fonte: The Record, 16/11

ISRAEL · FORNECEDOR DE SEGURANÇA

Radware informa acesso indevido a API do Cloud WAF e orienta troca de chaves

A Radware avisou clientes que, em 19/11, alguém acessou uma API interna de gestão do Cloud WAF que estava exposta sem autenticação; o acesso foi detectado cerca de 10 horas depois. Podem ter sido expostos dados de contato e, para parte dos clientes, credenciais de exportação de logs para AWS S3, Azure Blob ou SFTP.

A empresa diz que a proteção do WAF, o tráfego, os certificados e a defesa contra DDoS não foram afetados. Quem usa o serviço deve trocar as chaves de exportação de logs e revisar os acessos aos buckets desde 19/11.

Fonte: BleepingComputer, 24/11

⚠ Alerta: falhas exploradas agora

PRIORIDADE PARA BORDA E FERRAMENTAS DE GESTÃO

Drupal core abaixo de 10.6.22, 11.3.22 e 11.4.13

CVE-2026-132165 (SA-CORE-2026-017) — no KEV da CISA desde 24/11/2026, prazo 27/11/2026

Em 24/11 a CISA incluiu no catálogo de falhas exploradas (KEV) a falha do instalador do Drupal, corrigida em 18/11 (aviso SA-CORE-2026-017). O instalador continua no site depois da instalação e pode permitir que alguém sem login assuma o site; até então só havia prova de conceito.

A CISA não detalhou quem explora nem os alvos. Relevante para portais públicos e institucionais feitos em Drupal; o prazo para os órgãos federais dos EUA é 27/11.

O QUE FAZER

1. Atualizar para Drupal 11.4.13, 11.3.22 ou 10.6.22.
2. Bloquear o acesso a /core/install.php no servidor web, mesmo após atualizar.
3. Garantir que o servidor web não consiga gravar nem mudar permissões do settings.php; versões sem suporte (≤11.2, ≤10.5, 8 e 9) não terão correção.

Fontes: The Hacker News, 19/11 · Nota oficial: Drupal Security Team — SA-CORE-2026-017, 18/11 · Nota oficial: CISA — catálogo KEV, 24/11

Azure API Management (Classic)

sem CVE divulgado

Um ator desconhecido explorou uma falha no Azure API Management (instâncias Classic) para tentar extrair tokens de acesso, segredos e named values. A Microsoft identificou o problema em 18/11 e fechou o caminho de acesso no dia seguinte.

A autoridade norueguesa NSM diz que várias empresas do país foram atingidas, entre elas Equinor e Skagerak Energi, e que houve vítimas também fora da Noruega; a extensão ainda não é clara. Camadas v2 e Consumption não são afetadas.

O QUE FAZER

1. Tratar como comprometidos e trocar todos os tokens, segredos e named values do APIM.
2. Mapear quais dados e APIs ficam atrás da instância para medir o possível impacto.
3. Conferir na página de status do gateway se a versão já está corrigida (0.52.x a partir do build 31936; 0.53.x a partir do build 31938); se não, acionar a Microsoft.

Fontes: Nota oficial: NSM (Noruega) — medidas contra vulnerabilidade no Azure API Management, 23/11 · SecurityWeek, 23/11

Optimizely Web Experimentation (serviço em nuvem)

CVE-2026-132224 — KEV da CISA em 24/11/2026, prazo 27/11/2026

A CISA incluiu no KEV a falha no fluxo de cadastro do Optimizely Web Experimentation que deixava um atacante se passar por usuários de clientes e alterar o JavaScript dos projetos. É a falha usada na injeção de código malicioso em sites de grandes marcas em 16/11.

O código circulava pelos arquivos hospedados pela própria Optimizely e rodava no navegador de quem visitava os sites afetados. A Optimizely diz já ter corrigido no servidor.

O QUE FAZER

1. Se o site usa Optimizely Web Experimentation: revisar o JavaScript de projetos e mudanças feitas desde 16/11 e os usuários da conta.
2. Seguir o relatório de incidente da Optimizely e revogar/recriar tokens e acessos da conta.
3. Adotar CSP e SRI para scripts de terceiros nos portais; conferir pagamentos e transações feitos em 16/11.

Fontes: Nota oficial: CISA — catálogo KEV, 24/11 · Nota oficial: Optimizely — relatório de incidente (17/11), 17/11 · Bitsight, 24/11

Método: notícias públicas, rastreadores e as notas dos próprios afetados (fabricantes, órgãos, empresas, CVM, ANPD, CTIR Gov), com o link de cada fonte junto do texto; nenhum site de vazamento ou fórum criminoso foi acessado. Os textos são paráfrases. Conteúdo informativo, produzido com apoio de inteligência artificial a partir de fontes públicas. Alegações de grupos criminosos não foram confirmadas pelas vítimas. Correções e atualizações são publicadas nas edições seguintes.

Receba o Radar todo dia útil

Inovação, Ciberataques, Cidades e Governo Digital e Investimentos em TI por e-mail ou no canal do WhatsApp. É grátis, e você cancela quando quiser.

Inscreva-se: hubterritory.com/radar/inscricao