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 11

Radar de Ciberataques

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

Quinta-feira, 26 de novembro de 2026 Janela: qua 25/11, 07h06 a qui 26/11, 06h57 Edição nº 11

1	1	3
CASOS NO BRASIL	CONFIRMADOS	FALHAS EXPLORADAS

BRASIL · BANCO PÚBLICO

Banpará detecta fraude via Pix em conta do governo do Pará e informa recuperação dos valores

Cerca de 600 transferências, que somavam aproximadamente R$ 8,5 milhões segundo a apuração inicial, saíram de uma conta da Secretaria da Fazenda em 23/11; o banco bloqueou os acessos, comunicou o Banco Central e a Polícia Civil investiga. No mundo, a FinCEN, do Tesouro dos EUA, tirou sistemas do ar por precaução, e Palo Alto e Juniper corrigiram falhas exploradas em equipamentos de rede.

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.

BANCO ESTADUAL · PA/BELÉM

Cerca de 600 Pix indevidos saem de conta da Fazenda do Pará; Polícia Civil investiga

CONFIRMADO EM ANDAMENTO Banpará / conta da Secretaria da Fazenda do Pará · fraude com transferências Pix; forma de acesso não divulgada

Na noite de 23/11, os controles do Banpará identificaram movimentações atípicas numa conta transitória da Secretaria da Fazenda do Pará: cerca de 600 transferências via Pix, que somavam aproximadamente R$ 8,5 milhões segundo a apuração inicial, para contas em outras instituições.

Em nota, o banco informou que bloqueou os acessos, que seus controles permitiram recuperar os valores e que comunicou o Banco Central; a Polícia Civil investiga. O valor efetivamente recuperado e a forma de acesso à conta não foram divulgados.

O que outros órgãos podem fazer: definir limites e alertas para transferências fora do padrão em contas públicas, exigir MFA e revisar com frequência quem pode movimentá-las, e ter um plano para acionar o banco e as instituições de destino nas primeiras horas.

Fontes: O Liberal, 24/11 · Estado do Pará Online (com nota do Banpará via Agência Pará), 25/11

CORRIJA TAMBÉM · FALHAS EXPLORADAS

Mitel MiCollab e GeoServer também têm falhas exploradas

Mitel MiCollab: cinco falhas do componente de conferência AWV entraram em 25/11 no catálogo KEV da CISA (prazo 28/11; uma delas, 9/12); a mais grave permite executar comandos no servidor sem login (CVSS 10). Aplicar o patch do aviso MISA-2026-0012 para a versão 10.3 ou bloquear o acesso externo ao AWV.

GeoServer: segundo a watchTowr, citada pelo The Hacker News, duas falhas recém-corrigidas já são exploradas (leitura de arquivos sem login via WFS e acesso a operações protegidas); combinadas a outras, permitem executar código no servidor. Muito usado por prefeituras e órgãos de geoinformação: atualizar para 2.27.7, 2.28.6 ou 3.0.2, ou restringir o WFS anônimo.

Fontes: Nota oficial: CISA — catálogo KEV (cópia oficial no GitHub), 25/11 · Nota oficial: Mitel — MISA-2026-0012, 16/11 · Nota oficial: GeoServer — aviso GHSA-39mw-5chv-jh47, 23/11 · The Hacker News, 25/11

Atualizações CASOS DE EDIÇÕES ANTERIORES QUE MUDARAM

Portal do Governo de Alagoas: retorno ainda sem data. Em 25/11, o portal institucional seguia fora do ar à espera da nova plataforma anunciada pelo Itec, sem nova data; segundo o instituto, só o portal foi atingido e o conteúdo será recuperado de backup. Lição: MFA e revisão periódica das contas de administrador de portais.

Fonte: Frances News (CadaMinuto), 25/11

ARTEX no arsenal de grupos estatais. Em 25/11, a Microsoft disse que grupos estatais chineses (como Salt Typhoon) e norte-coreanos, além de grupos financeiros, incorporaram a ferramenta de IA ARTEX para reconhecimento, ataque a credenciais e exploração de aplicações web. Recomenda MFA resistente a phishing para administradores, WAF e detecção de requisições em ritmo de máquina.

Fontes: Nota oficial: Microsoft Security Blog, 25/11 · The Record, 25/11

Novo site de extorsão INCEPTION. O INCEPTION nega vínculo com o ShinyHunters, e uma conta ligada ao ShinyHunters anunciou em 24/11 a volta do grupo, possivelmente um impostor. As vítimas listadas não tiveram a autenticidade verificada.

Fonte: SecurityWeek, 25/11

Drupal: exploração confirmada no instalador. O aviso SA-CORE-2026-017 registra exploração em sites desde 19/11; em 25/11 o Drupal publicou uma nova falha correlata, também explorada (SA-CORE-2026-019, no Alerta desta edição).

Fonte: Nota oficial: Drupal Security Team — SA-CORE-2026-017, 18/11

Xen Orchestra entra no catálogo KEV. O contorno de autenticação do aviso VSA-2026-062 recebeu a CVE-2026-133469 e entrou em 25/11 no catálogo KEV da CISA, com prazo até 28/11 para órgãos federais dos EUA. Atualizar para 6.9.2 ou 6.10.1 e manter o console fora da internet.

Fontes: Nota oficial: Vates (aviso VSA-2026-062), 10/11 · Nota oficial: CISA — catálogo KEV (cópia oficial no GitHub), 25/11

Mundo

OS CASOS MAIS RELEVANTES DO PERÍODO

EUA · GOVERNO FEDERAL

FinCEN, do Tesouro dos EUA, tira sistemas do ar após invasão

A FinCEN, órgão do Tesouro americano que recebe os relatórios da Lei de Sigilo Bancário (como comunicações de operações suspeitas), informou acesso não autorizado a uma parte limitada de seus sistemas e tirou alguns do ar por precaução, segundo The Hacker News.

Provedores de envio relatam falhas nos envios automáticos em lote desde 18/11. Em 24/11 a FinCEN publicou a ordem FIN-2026-R002, que cita uma 'interrupção de serviço' e dá prazo até 30/12 para relatórios que venceriam entre 18/11 e 29/12 a quem usa o canal SDTM, além de relatórios de beneficiário final.

O órgão não disse quais sistemas foram afetados, se houve acesso ou roubo de dados, nem quem está por trás; nenhum grupo reivindicou.

Fontes: Nota oficial: FinCEN — Ordem FIN-2026-R002, 24/11 · The Hacker News, 25/11

FRANÇA/GUADALUPE · SAÚDE PÚBLICA

Hospital universitário de Guadalupe suspende cirurgias e radioterapia após suspeita de ransomware

Falhas em computadores e telefones surgiram na noite de 21/11 no CHU da Guadalupe, que atende cerca de 380 mil habitantes. Cirurgias, consultas e exames de imagem foram cancelados ao menos até sexta, a radioterapia foi suspensa e sessões de quimioterapia foram canceladas; emergência, diálise e casos cardíacos urgentes seguem atendidos.

A ANSSI, agência francesa de cibersegurança, diz que o caso parece envolver ransomware e apura se a entrada foi por um fornecedor de TI; a promotoria de Paris investiga. O hospital diz não ter recebido pedido de resgate.

Lição para hospitais públicos: plano de contingência clínico ensaiado, backups isolados e revisão dos acessos de fornecedores de TI.

Fonte: The Record, 25/11

SUÍÇA E ITÁLIA · INFRAESTRUTURA CRÍTICA

Suíça e Itália relatam invasões conduzidas por agentes de IA

O centro nacional de cibersegurança da Suíça (NCSC) informou em 24/11 os primeiros casos no país de ataques feitos com ajuda de agentes de IA: organizações e operadores de infraestrutura crítica de ao menos dois setores, e em todos os casos conhecidos os sistemas foram comprometidos. Os agentes exploraram senhas fracas e falhas conhecidas em sistemas expostos à internet e mudavam de método quando havia reação.

A CSIRT Italia relatou campanhas em larga escala com vários agentes trabalhando em paralelo, que comprometeram muitos sistemas em poucas horas, segundo o BleepingComputer. Nenhum dos dois órgãos identificou vítimas; o NCSC diz que o número de agentes ofensivos acessíveis pela internet quase dobrou desde outubro.

Recomendações do NCSC: reduzir sistemas expostos, aplicar patches críticos de sistemas de internet em até 24 horas, exigir MFA ou passkeys em todo acesso pela internet, usar menor privilégio e monitorar mudanças anormais de comportamento e de volume de dados.

Fontes: Nota oficial: NCSC/BACS (Suíça) — aviso oficial, 24/11 · BleepingComputer, 25/11 · Minuto da Segurança, 26/11

GLOBAL · GERENCIADOR DE SENHAS

1Password confirma invasão via conta GitHub de funcionário e exposição de dados de clientes

A 1Password informou em 25/11 que um atacante invadiu a conta corporativa do GitHub de um funcionário (investigação aberta em 19/11), copiou código-fonte de repositórios privados, acessou o sistema de CI/CD e enviou código malicioso a serviços de backend, que baixou dados administrativos de parte dos usuários.

Foram expostos nomes, e-mails, identificadores de conta, chaves públicas, parâmetros SRP e tokens de alguns e-mails de convite e recuperação. Segundo a empresa, cofres, senhas-mestras e Secret Keys não foram acessados; credenciais internas foram rotacionadas.

O que fazer: nenhuma ação obrigatória na conta; alertar usuários corporativos para phishing com falsos convites ou pedidos de recuperação da 1Password.

Fontes: Nota oficial: 1Password — blog oficial, 25/11 · The Hacker News, 26/11

HONG KONG · GOVERNO

Invasão a sistema de ingressos do governo de Hong Kong pode ter exposto dados de 1,3 milhão de contas

O departamento de lazer e cultura de Hong Kong informou em 25/11 que hackers invadiram o Urbtix, sistema de venda de ingressos on-line operado por uma empresa terceirizada, que avisou o órgão em 24/11. O caso foi levado à polícia e à autoridade de proteção de dados.

Podem ter sido expostos nome de usuário ou nome completo, telefone e e-mail de cerca de 1,3 milhão de contas; segundo o órgão, a base não guarda documento de identidade e os dados de cartão ficam mascarados. O sistema segue funcionando.

Lição: contratos de sistemas públicos operados por terceiros devem prever controles de acesso, monitoramento e prazo curto para avisar o órgão.

Fonte: Dimsum Daily, 25/11

⚠ Alerta: falhas exploradas agora

PRIORIDADE PARA BORDA E FERRAMENTAS DE GESTÃO

Palo Alto Networks PAN-OS (firewalls)

CVE-2026-46300 (Fragnesia, kernel Linux), explorada em cadeia com CVE-2026-109618 (PHP2Shell); fora do KEV até o catálogo de 24/11

A Palo Alto publicou o boletim PAN-SA-2026-0015 com correções no PAN-OS para a CVE-2026-46300 ('Fragnesia'), falha de escalada de privilégio no kernel Linux, e diz ter observado exploração contra interfaces de gerenciamento expostas à internet.

Segundo a SecurityWeek, um grupo de língua chinesa encadeou a PHP2Shell (acesso inicial, já corrigida até 30/10) com a Fragnesia para obter root, atingindo 25 servidores — 24 firewalls e um servidor interno de gerência. O único vetor conhecido exige antes explorar a PHP2Shell pela interface de gerenciamento exposta.

O QUE FAZER

1. Atualizar o PAN-OS para versão corrigida: 10.2.7-h41/10.2.10-h45/10.2.13-h29/10.2.16-h14/10.2.18-h15; 11.1.4-h40/11.1.6-h42/11.1.7-h14/11.1.10-h38/11.1.13-h18/11.1.16-h6; 11.2.4-h25/11.2.7-h25/11.2.10-h19/11.2.13-h6/11.2.16-h3; 12.1.4-h15/12.1.7-h15/12.1.10-h6; 12.2.4-h3 (ou posteriores).
2. Confirmar que a correção da PHP2Shell (CVE-2026-109618) já está aplicada.
3. Tirar a interface de gerenciamento (e perfis de gerência em interfaces de dataplane) da internet; permitir só IPs internos confiáveis ou VPN.
4. Se a gerência esteve exposta, revisar logs e sinais de comprometimento.

Fontes: Nota oficial: Palo Alto Networks — PAN-SA-2026-0015, 24/11 · Nota oficial: Palo Alto Networks — aviso CVE-2026-109618 (PHP2Shell), 30/10 · SecurityWeek, 25/11

HPE Juniper Session Smart Router e Session Smart Conductor (SD-WAN)

CVE-2026-103406 (CVSS 9,8) · KEV desde 25/11/2026 · prazo CISA 28/11/2026

A CISA incluiu em 25/11 no catálogo KEV a CVE-2026-103406, injeção de comando nos roteadores SD-WAN Session Smart da Juniper (HPE): um atacante remoto, sem login, executa comandos como root por meio de um ID de 'salt minion' manipulado. O prazo para órgãos federais dos EUA é 28/11.

A correção saiu no boletim de outubro da Juniper (versões 7.0.5, 7.1.7 e 7.2.3). Segundo a SecurityOnline, a Juniper atualizou o aviso em 24/11 para confirmar ao menos um caso de exploração maliciosa relatado ao seu time de resposta.

O QUE FAZER

1. Atualizar Session Smart Router/Conductor para 7.0.5, 7.1.7 ou 7.2.3 (ou posterior); a Juniper diz que não há contorno.
2. Atualizar primeiro o Conductor e depois os roteadores gerenciados.
3. Restringir o acesso de gerência e o canal de gestão de chaves (salt) a redes confiáveis.
4. Revisar logs em busca de comandos inesperados como root; a CISA pede triagem forense dos ativos expostos.

Fontes: Nota oficial: CISA — catálogo KEV (cópia oficial no GitHub), 25/11 · Nota oficial: Juniper — boletim Session Smart Router/Conductor (out/2026), 28/10 · SecurityOnline, 28/10

Drupal core 10.x e 11.x

CVE-2026-136716 (SA-CORE-2026-019, 'altamente crítica', 21/25) — exploração confirmada pelo Drupal; fora do KEV da CISA até o catálogo de 25/11

O Drupal publicou em 25/11 o aviso SA-CORE-2026-019: sites que ficaram em estado de instalação incompleto ou incomum continuavam vulneráveis a tomada pelo install.php mesmo após a correção anterior (SA-CORE-2026-017, já explorada). O aviso diz que a nova falha é explorada ativamente; o estado vulnerável não aparece no painel e sites já invadidos podem não parecer vulneráveis.

Afeta Drupal 10 antes de 10.6.23 e Drupal 11 antes de 11.3.23 e 11.4.14. O Centro Canadense de Cibersegurança repercutiu o aviso (AV26-1209).

O QUE FAZER

1. Atualizar para 11.4.14, 11.3.23 ou 10.6.23 e rodar o update.php (o hook de atualização corrige sites já em produção nesse estado).
2. Bloquear o acesso ao install.php em todos os sites, seguindo o guia do Drupal.
3. Revisar logs do usuário 1 (admin): mudanças inesperadas, e-mail que não seja seu; trocar a senha do usuário 1.
4. Versões 11.2.x, 10.5.x e anteriores (e Drupal 8/9) estão sem suporte: migrar.

Fontes: Nota oficial: Drupal — SA-CORE-2026-019, 25/11 · Nota oficial: Centro Canadense de Cibersegurança — AV26-1209, 25/11

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