Radar de Ciberataques

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

Quinta-feira, 19 de novembro de 2026 Janela: qua 18/11, 07h06 a qui 19/11, 06h57 Edição nº 6

2	2	3
CASOS NO BRASIL	CONFIRMADOS	FALHAS EXPLORADAS

BRASIL · BANCO PÚBLICO

Banco do Brasil informa acesso indevido a dados cadastrais de clientes

O banco diz que uma credencial válida foi usada por terceiros e já foi revogada, sem acesso a senhas nem movimentações indevidas. A Prefeitura de Colorado (RS) também comunicou um incidente em contas bancárias do município.

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 PÚBLICO · NACIONAL

Banco do Brasil informa acesso indevido a dados cadastrais de clientes

CONFIRMADO EM ANDAMENTO Banco do Brasil · acesso não autorizado com credencial válida; sem grupo identificado

O Banco do Brasil informou a correntistas, em 18/11, que identificou em 12/11 o acesso indevido a informações cadastrais de clientes por meio de uma credencial válida usada por terceiros. A credencial já foi revogada.

Segundo o banco, podem ter sido expostos nome, CPF, e-mail, agência e, em alguns casos, número da conta; senhas e códigos de segurança não foram afetados e não foram encontradas movimentações indevidas. O número de clientes envolvidos não foi divulgado, e o banco diz que fará as notificações previstas na LGPD.

Para outras instituições: o uso de credenciais legítimas é difícil de separar do uso normal. Autenticação multifator, revisão periódica dos acessos de funcionários e parceiros e alertas para consultas em volume fora do padrão ajudam a detectar esse tipo de caso mais cedo.

Fontes: Convergência Digital, 18/11 · Exame, 18/11

PREFEITURA · RS / COLORADO

Prefeitura de Colorado (RS) comunica movimentações não autorizadas em contas do município

CONFIRMADO EM ANDAMENTO Prefeitura de Colorado (RS) · acesso indevido a contas bancárias do município; forma de acesso não divulgada

A Prefeitura de Colorado (RS) informou um ataque cibernético envolvendo contas bancárias do município na Caixa Econômica Federal, com movimentações financeiras não autorizadas, segundo o Grupo Ceres de Comunicação (18/11). A prefeitura comunicou a polícia e o banco e apura o caso.

Valores, data e forma de acesso às contas não foram divulgados.

Para outros municípios: autenticação multifator e dupla aprovação para pagamentos e transferências, um computador usado só para o internet banking, limites e alertas de movimentação combinados com o banco e revisão periódica de quem tem acesso às contas reduzem o risco desse tipo de fraude.

Fonte: Grupo Ceres de Comunicação, 18/11

CORRIJA TAMBÉM

Outras correções críticas: Apache Roller, Java, NGINX, F5 e PHP

Apache Roller (CVE-2026-129448): a Apache confirmou exploração ativa da falha, que permite executar código sem login pelo XML-RPC; a correção está na versão 6.1.6. Java (Java4Shell, CVE-2026-114938): a CISA pediu correção imediata em 17/11; afeta Java 17 a 27 e produtos como Keycloak, Jira e Jenkins, ainda sem exploração confirmada.

NGINX (CVE-2026-123007, no HTTP/2) e F5 BIG-IP (seis falhas no plano de dados) ganharam correções em 18/11; há provas de conceito públicas para o NGINX e nenhum ataque relatado. O PHP publica hoje, 19/11, entre 11h e 11h30 (Brasília), versões de segurança para todas as versões suportadas.

Fontes: Nota oficial: Apache — aviso CVE-2026-129448, 18/11 · Nota oficial: CISA — alerta Java4Shell, 17/11 · Nota oficial: NGINX — avisos de segurança, 18/11 · Nota oficial: F5 — K000164058, 18/11 · Nota oficial: PHP.net, 18/11

Atualizações

CASOS DE EDIÇÕES ANTERIORES QUE MUDARAM

Porto de Santos (APS): Em 17/11, a Autoridade Portuária reuniu cerca de 60 representantes de terminais e entidades, apresentou a cronologia do incidente e criou um e-mail para relatos de problemas. Segundo a DatamarNews, a invasão apagou dados e a restauração dos serviços administrativos segue gradual, sem efeito na movimentação de carga.

Fontes: Gazeta do Povo, 13/11 · DatamarNews, 18/11

N-able N-central: A CISA incluiu em 18/11 no catálogo de falhas exploradas (KEV) a falha do Apache Axis usada na cadeia de ataque ao N-central (CVE-2026-90436), com prazo até 21/11. A orientação segue: aplicar o N-central 2026.4 HF3 e atualizar agentes e probes.

Fontes: Nota oficial: N-able (atualização oficial de correções), 16/11 · Nota oficial: CISA KEV (catálogo oficial, GitHub), 18/11

Mundo

OS CASOS MAIS RELEVANTES DO PERÍODO

JAPÃO · SUPERCOMPUTADOR

Japão suspende o supercomputador Fugaku após acesso não autorizado

O instituto público japonês RIKEN informou que um invasor acessou, de 10 a 13/11, a rede de operação do supercomputador Fugaku a partir de um painel web público de status. Nomes, e-mails e IDs de até 4.222 usuários do Fugaku e 375 do sistema Rikyu, além de chaves SSH e de acesso guardadas nos diretórios pessoais, podem ter sido expostos. O Fugaku está parado desde 14/11 e as chaves foram trocadas.

Lição para outros órgãos: painéis e interfaces web expostos à internet, mesmo os só informativos, precisam estar atualizados e isolados da rede interna, e credenciais guardadas em servidores compartilhados devem ser trocadas periodicamente.

Fontes: Nota oficial: RIKEN — aviso oficial de 16/11, 16/11 · BleepingComputer, 17/11 · SDxCentral, 16/11

ÁSIA · ESPIONAGEM EM GOVERNOS

Grupo suspeito de ligação com a China renova malware usado contra o governo das Filipinas

A Bitdefender relatou que o grupo por trás do malware EggStreme reescreveu a ferramenta depois de exposto em 2025 e segue mirando órgãos do governo filipino, com indícios de ações contra Taiwan. A nova versão ganhou reconhecimento de Active Directory, uso de PowerShell e uma variante que apenas escuta numa porta.

Para órgãos públicos, monitorar o uso de PowerShell e consultas incomuns ao Active Directory ajuda a detectar esse tipo de espionagem.

Fonte: The Hacker News, 18/11

EUA · RANSOMWARE

Grupo de ransomware diz ter dados da Nvidia; empresa não comentou

O grupo The Gentlemen incluiu a Nvidia em sua lista de vítimas e ameaça publicar dados em cerca de dez dias, segundo o Times Brasil. Não há amostra de arquivos nem detalhe da área supostamente afetada, e a Nvidia não confirmou nem negou. A alegação não foi verificada.

Fonte: Times Brasil, 18/11

⚠ Alerta: falhas exploradas agora

PRIORIDADE PARA BORDA E FERRAMENTAS DE GESTÃO

Synology DiskStation Manager (DSM) e BeeStation OS

CVE-2024-10441 (CVSS 9,8) — KEV da CISA em 18/11/2026, prazo 21/11/2026

A CISA incluiu em 18/11 no catálogo de falhas exploradas (KEV) uma brecha no daemon de plugins do sistema do Synology DSM que permite a um atacante remoto executar código. A falha é de 2024 e já tinha correção da Synology.

O prazo dado aos órgãos federais americanos é curto (21/11), sinal de urgência. NAS como esse são comuns em escritórios, empresas e órgãos públicos; os que têm a administração aberta à internet correm mais risco.

O QUE FAZER

1. Atualizar o DSM para 7.2-64570-4, 7.2.1-69057-6 ou 7.2.2-72806-1 (ou posterior); BeeStation OS para 1.1-65374 ou posterior.
2. Tirar a interface de administração do NAS da internet (acesso só por VPN).
3. Verificar sinais de comprometimento em NAS que ficaram expostos sem atualização.

Fontes: Nota oficial: CISA KEV (catálogo oficial, GitHub), 18/11 · Nota oficial: Synology Security Advisory SA_24_20, 27/03

REDCap (Vanderbilt University)

CVE-2026-90817 (CVSS 9,8) — KEV da CISA em 18/11/2026, prazo 21/11/2026

A CISA incluiu em 18/11 no KEV uma falha do REDCap, plataforma de coleta de dados de pesquisa clínica usada por hospitais e universidades, inclusive públicas. Basta conhecer o código de um questionário público para executar código no servidor sem login.

Em junho, o Google relatou que o grupo chinês UNC6508 mira servidores REDCap desatualizados para espionagem; a Censys contou cerca de 8.500 instâncias expostas, a maioria sem a versão mais recente.

O QUE FAZER

1. Atualizar para REDCap 16.0.49 LTS, 17.3.10 LTS ou 17.4.4 Standard (ou posterior).
2. Remover versões legadas que ficam rodando lado a lado no servidor.
3. Revisar logs de importação de dados e questionários públicos em busca de acessos estranhos.

Fontes: Nota oficial: CISA KEV (catálogo oficial, GitHub), 18/11 · OpenCVE (registro da CVE), 20/09 · SecurityWeek, 18/06

BerriAI LiteLLM (proxy/gateway de LLM)

CVE-2026-40217 (CVSS 8,8) — KEV da CISA em 18/11/2026, prazo 02/12/2026

A CISA incluiu em 18/11 no KEV uma falha do LiteLLM, gateway usado por empresas para centralizar acesso a modelos de IA. O endpoint de teste de guardrails permite escapar do sandbox e executar código no servidor.

A Zenity Labs registrou em honeypots, entre abril e maio de 2026, tentativas reais: varredura, força bruta de chaves mestras padrão (como sk-1234) e payloads que leem chaves de API e executam comandos. A imagem Docker padrão roda como root.

O QUE FAZER

1. Atualizar o LiteLLM para 1.83.10 ou superior.
2. Trocar a chave mestra padrão por uma forte e tirar o plano de controle da internet.
3. Usar a imagem não root e alertar qualquer POST externo para /guardrails/test_custom_code.

Fontes: Nota oficial: CISA KEV (catálogo oficial, GitHub), 18/11 · Nota oficial: BerriAI LiteLLM — advisory GHSA-wxxx-gvqv-xp7p, 15/04 · Zenity Labs, 30/06

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.