Radar de Ciberataques

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

Quarta-feira, 18 de novembro de 2026 Janela: ter 17/11, 07h05 a qua 18/11, 06h57 Edição nº 5

1	1	3
CASOS NO BRASIL	CONFIRMADOS	FALHAS EXPLORADAS

BRASIL · ÓRGÃO FEDERAL

Inep relata tentativas de ataque ao site no 2º dia do Enem

Segundo o ministro da Educação, as tentativas foram acompanhadas por uma equipe de monitoramento, sem relato de impacto na prova. No mundo, ataques por meio de fornecedores atingiram Optimizely, Expedia e Uber.

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.

ÓRGÃO FEDERAL · DF / BRASÍLIA

Inep relata tentativas de ataque ao site no 2º dia do Enem

CONFIRMADO Inep (Instituto Nacional de Estudos e Pesquisas Educacionais) · tentativas de ataque ao site; tipo não divulgado

No domingo, 15/11, segundo dia de provas do Enem, o ministro da Educação disse, durante visita à sede do Inep em Brasília, que a página do instituto vinha sendo alvo de tentativas de ataque hacker e que a equipe acompanhava a situação numa sala de monitoramento montada para o exame.

Não foram divulgados o tipo de ataque, o número de tentativas nem se o site ficou instável; não há relato de impacto na aplicação da prova nem de vazamento de dados.

Para outros órgãos: datas de grande audiência atraem ataques. Reforçar a proteção contra negação de serviço, manter monitoramento dedicado no período e ter plano de contingência para os serviços on-line reduz o risco.

Fontes: Times Brasil (CNBC), 15/11 · Gazeta do Povo, 15/11

EUA · INTELIGÊNCIA

Rede interna sigilosa da NSA sai do ar; fontes não veem sinal de ataque

A NSA Net, rede que a NSA usa para trocar informações classificadas internamente, ficou indisponível em 17/11, segundo seis fontes ouvidas pela CNN; a agência escalonou a chegada de funcionários à sede.

Segundo as fontes, não há até agora evidência de ciberataque; causa, alcance e prazo de retorno não foram divulgados. É mais uma pane numa série recente nos EUA (Microsoft 12/11, FAA 13/11, bancos 16/11), sem ligação comprovada entre elas.

Fontes: CP24 (repercute CNN), 17/11 · InfoMoney, 17/11

Atualizações CASOS DE EDIÇÕES ANTERIORES QUE MUDARAM

Mercado Bitcoin reabre o Pix. Em 17/11 a corretora liberou depósitos via Pix e saques em reais só para conta do mesmo CPF, após nova validação no app. Compra, venda e transferência de cripto seguem suspensas, sem data.

Fonte: AVNews (Ativo Virtual), 17/11

ScreenConnect: ataques seguem em servidores locais. A ConnectWise concluiu a investigação em 16/11: os ataques continuam em instalações locais com extensões de terceiros ativas e sem atualização, ligados à falha CVE-2026-84869 (CVSS 9,9). Recomenda cliente técnico 26.6.5 ou superior e não reativar as extensões.

Fontes: Nota oficial: ConnectWise (avisos oficiais), 16/11 · The Hacker News, 17/11

Caso Fireworks AI: Uber informa 149.346 afetados. A Uber notificou autoridades nos EUA de que credenciais de um fornecedor deram acesso a um ambiente de nuvem com nome, endereço, nascimento e imagem da carteira de motorista de 149.346 pessoas. A empresa não nomeou o fornecedor; a imprensa o liga à Fireworks AI, origem do ataque ao Cursor.

Fontes: The Record, 17/11 · SecurityWeek, 16/11

Paralisação da FAA: troca de cabos, não ataque. O secretário de Transportes dos EUA atribuiu a parada de 13/11 a uma troca de linhas de cobre por fibra feita pela contratada L3Harris; a FAA disse não ver ação maliciosa. O erro exato segue em investigação.

Fontes: Nota oficial: WGCU/NPR — coletiva do secretário de Transportes, 14/11 · SecurityWeek, 14/11

Mundo

OS CASOS MAIS RELEVANTES DO PERÍODO

EUA · CADEIA DE SUPRIMENTOS

Invasão na Optimizely injeta código malicioso em sites de grandes marcas

A Optimizely confirmou que um terceiro explorou uma falha no cadastro de contas do Experimentation para inserir JavaScript malicioso em projetos de clientes. Um pesquisador independente achou 188 arquivos infectados de 178 organizações, com sites como Zoom, CNN, BBC, Salesforce, GitLab, KLM e Air France entre os citados; a primeira injeção foi na madrugada de 16/11.

O script carregava código externo que troca endereços de carteira cripto, captura dados de cartão, coleta cookies e entrega kits de exploit para iPhone. A empresa diz ter corrigido a falha, removido o código e revogado tokens; a Salesforce desligou os scripts da Optimizely. Lição: revisar scripts de terceiros nos portais (CSP/SRI) e conferir pagamentos e transferências feitos em 16/11.

Fontes: Nota oficial: Optimizely (página de status oficial), 17/11 · BleepingComputer, 16/11

EUA · TURISMO · CADEIA DE SUPRIMENTOS

Expedia confirma invasão via fornecedor; n0n alega quase 1 bilhão de registros

A Expedia confirmou que invasores chegaram a seus sistemas por meio de um fornecedor terceirizado de plataforma de dados, num ataque que atingiu também outras empresas; diz que a investigação segue e que as plataformas estão seguras.

O grupo n0n alega ter levado mais de 830 milhões de registros de fidelidade, 333 milhões de registros de contas/credenciais (com hash) e código-fonte; a Expedia não confirmou os números. Wiz e Sentra ligam o acesso a uma chave roubada da Qubole, parceira do Google Cloud.

Recomendação: trocar senhas de Expedia, Hotels.com e Vrbo e esperar phishing com dados de fidelidade.

Fontes: Security Affairs, 14/11 · Skift, 12/11

GLOBAL · PHISHING MICROSOFT 365

Golpe usa o apagão real do Microsoft 365 como isca para roubar senhas

A Microsoft confirmou que a queda do Microsoft 365 de 12 e 13/11 foi falha técnica, ligada a uma mudança de capacidade de rede, e não ataque. Logo depois, sua equipe de inteligência alertou para e-mails falsos que imitam avisos de saúde do serviço e citam o número real do incidente (EX1550543).

As mensagens dizem que e-mails retidos durante a queda serão apagados em 24 horas se o usuário não clicar no link; os assuntos começam com "Outage -". A Microsoft diz que a atividade é compatível com roubo de credenciais, mas a coleta de senhas não foi confirmada, e que seus produtos já bloqueiam a campanha. Vale alertar usuários de órgãos que usam o Microsoft 365, como o Judiciário, afetado pela queda.

Fontes: SecurityWeek, 16/11 · Nota oficial: Microsoft Threat Intelligence (post citado pela SecurityWeek), 16/11

ROMÊNIA · ESPIONAGEM

Romênia atribui ao grupo russo Turla invasão a e-mail de órgão do governo

O serviço de inteligência da Romênia (SRI) divulgou em 11/11 que um órgão de governo não identificado teve o servidor de e-mail invadido para interceptar mensagens trocadas com a OTAN e a UE. A intrusão foi detectada em dezembro de 2025, contida e os sistemas restaurados; segundo o SRI, não se identificou exfiltração de dados sensíveis.

A operação foi atribuída ao Turla, grupo ligado ao FSB, que explorou falhas em sistemas Microsoft. A ESET associa ao caso um kit novo, chamado Cereal, também usado contra servidores de e-mail do governo do Cazaquistão. Segundo o The Record (16/11), a Rússia nega a autoria.

Lição para órgãos públicos: manter servidores de e-mail atualizados e monitorar acessos e regras de encaminhamento fora do padrão.

Fontes: The Record, 12/11 · The Irish Times (Reuters), 11/11 · The Record (negativa da embaixada russa), 16/11

GLOBAL · CADEIA DE SUPRIMENTOS DE SOFTWARE

Pacote da Microsoft no PyPI é adulterado para roubar credenciais de nuvem

Duas versões do pacote agent-framework, da Microsoft, publicadas no PyPI em 17/11 com 33 minutos de intervalo (1.26.1 e 1.26.2), traziam um ladrão de credenciais que roda a cada início do Python, mesmo sem o pacote ser importado. Ele coleta variáveis de ambiente, arquivos de credenciais de nuvem e de desenvolvimento e tokens do Azure DevOps e de identidade gerenciada; a 1.26.2 também pega tokens OIDC do GitHub Actions.

As duas versões foram postas em quarentena; a reportagem não traz posição da Microsoft. Quem instalou deve isolar máquinas e runners afetados, voltar à 1.26.0 reconstruindo o ambiente e trocar as credenciais expostas a partir de um sistema limpo.

Fonte: The Hacker News, 18/11

⚠ Alerta: falhas exploradas agora

PRIORIDADE PARA BORDA E FERRAMENTAS DE GESTÃO

Check Point Security Gateway / Gaia OS

CVE-2026-123039 · encadeada com PHP2Shell (CVE-2026-109618 e CVE-2026-109619)

A exploração começou em 30/10: o invasor entra pelo portal Mobile Access usando as falhas do PHP, vira root no gateway, instala backdoor e salta para hosts VMware ESXi, onde roda um wiper que apaga dados. A Check Point viu exploração em cerca de duas dezenas de clientes.

O boletim oficial (sk1000362) lista como afetadas as versões R81 a R82.20; R81.10 e R81 estão fora de suporte e não têm correção. O relatório da Check Point Research (12/11) publica IOCs e cita uma segunda onda de varreduras em 2/11.

No Brasil, a Anatel já tinha tirado o SEI do ar de forma preventiva por causa do PHP2Shell em 21/10.

O QUE FAZER

1. Aplicar o Jumbo Hotfix com a correção (R82.20 Take 14, R82.10 Take 52, R82 Take 132 ou R81.20 Take 174, ou posteriores), começando pelos gateways com Mobile Access exposto.
2. Em R81.10 e R81 (sem correção) ou enquanto não aplicar: desativar o processo dynamic_server (paliativo) e planejar a migração de versão.
3. Procurar os IOCs publicados pela Check Point Research (hashes, IPs como 130.94.19[.]204) e acessos SSH do gateway para o ESXi.

Fontes: BleepingComputer, 13/11 · InvestNews, 23/10 · Nota oficial: Check Point (sk1000362), 12/11 · Nota oficial: Check Point Research, 12/11

N-able N-central (RMM)

CVE-2026-90436 · Apache Axis · CVSS 9.8 · cadeia "4EverAble2Shell"

Uma cadeia sem autenticação dá root no servidor que gerencia os endpoints dos clientes. Foram 21 servidores invadidos com minerador de cripto, 19 deles já com o Hotfix 2.

Em 16/11 a N-able publicou o N-central 2026.4 HF3, com 17 CVEs novas (CVE-2026-129271 a 129287) além das 7 do HF2; reforça autenticação e permissões, endurece a comunicação de agentes e probes e remove de vez a Legacy API. A empresa diz que ainda vai corrigir falhas de vazamento de dados que exigem acesso privilegiado.

O QUE FAZER

1. Aplicar o N-central 2026.4 HF3 (servidor) e atualizar Agents e Probes.
2. Manter a Legacy API desligada (o HF3 a remove).
3. Tratar qualquer indício como comprometimento total e acompanhar as próximas correções da N-able.

Fontes: The Hacker News, 13/11 · Nota oficial: N-able (atualização oficial de correções), 16/11 · The Hacker News, 17/11

Perforce Puppet Enterprise / Puppet Server; OpenVox

CVE-2026-115731 (CVSS 4.0: 9,4) — KEV da CISA em 17/11, prazo 01/12/2026; correlata CVE-2026-115732 (CVSS 9,0)

A CISA incluiu em 17/11 no catálogo KEV a CVE-2026-115731, falha de desserialização no processamento de relatórios do Puppet Server: um agente com certificado assinado pela CA pode executar código no servidor Puppet enviando um relatório adulterado.

Se a CA assina pedidos automaticamente (autosign) sem verificação forte, um atacante sem autenticação consegue o certificado e explora a falha. Há prova de conceito pública desde o início de novembro; a correlata CVE-2026-115732 (bypass de autorização por nome de certificado) já aparecia como explorada. A CISA cita relatos de exploração ativa, sem detalhar autores ou alvos.

O QUE FAZER

1. Atualizar Puppet Enterprise para 2023.8.13, 2025.12.1 ou 2026.0.1; Puppet Core 8.22.2 ou 9.1.3 (OpenVox: server 8.18.0 ou 9.2.0; agent 8.32.0 ou 9.3.0).
2. Até atualizar: restringir o acesso ao servidor Puppet só às redes necessárias.
3. Desativar ou endurecer o autosign da CA do Puppet.
4. Revisar regras personalizadas do auth.conf após o upgrade e procurar relatórios/execuções anômalas no servidor.

Fontes: Nota oficial: CISA — catálogo KEV (CVE-2026-115731), 17/11 · Nota oficial: Perforce — aviso de segurança (report deserialization code execution), 03/11 · SecurityOnline — PoC público para Puppet Server/OpenVox, 04/11 · The Hacker News, 18/11

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.