Radar de Ciberataques

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

Terça-feira, 17 de novembro de 2026 Janela: seg 16/11, 07h04 a ter 17/11, 07h05 Edição nº 4

2	2	1
CASOS NO BRASIL	CONFIRMADOS	FALHAS EXPLORADAS

BRASIL · SETOR PÚBLICO

Belo Horizonte confirma ataque ao sistema de guias e orienta contribuintes

Guias emitidas de 14 a 16/11 devem ser refeitas e os vencimentos passaram para 19/11. O TJMG confirmou o vazamento de alguns arquivos, e a falha explorada do dia atinge o console de virtualização Xen Orchestra.

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.

PREFEITURA · MG / BELO HORIZONTE

Prefeitura de BH confirma ataque ao sistema de guias e orienta contribuintes

CONFIRMADO EM ANDAMENTO Prefeitura de Belo Horizonte (PBH) · ataque cibernético ao sistema de emissão de guias; tipo não divulgado

A Prefeitura de Belo Horizonte informou na noite de 16/11 que um ataque cibernético afetou o sistema de emissão de guias de pagamento de tributos entre a madrugada de 14/11 e a manhã de 16/11. O serviço foi restabelecido, e a prefeitura diz ter contido o problema e acionado a polícia.

Guias emitidas nesse período não devem ser pagas: o contribuinte deve gerar outra pelo Portal de Serviços ou pelo app BH SIM. Código de barras e débito automático não foram afetados. Quem pagou por Pix deve conferir se o beneficiário é o Município de Belo Horizonte (ou o órgão arrecadador) e, se não for, procurar o banco e pedir o MED. Vencimentos entre 14 e 19/11 passaram para 19/11, sem juros e multa.

Para outros órgãos: manter monitoramento contínuo dos sistemas de arrecadação, inclusive fora do expediente; conferir automaticamente se o beneficiário das guias e dos QR Codes Pix é o próprio órgão; e ter pronto um aviso para contribuintes e bancos, como fez a prefeitura.

Fontes: Estado de Minas, 16/11 · O Tempo, 17/11 · Por Dentro de Minas, 16/11

PREFEITURA · MT / CUIABÁ

Cuiabá mantém UPAs em funcionamento com registro manual após tentativa de ataque

CONFIRMADO EM ANDAMENTO Prefeitura de Cuiabá (Secretaria Municipal de Saúde) · tentativa de ataque cibernético; tipo não divulgado

Em 3/11, a Prefeitura de Cuiabá informou que uma tentativa de ataque cibernético afetou o sistema da rede municipal de saúde. As UPAs seguiram atendendo, com registros e triagens feitos em papel, enquanto as equipes restabeleciam os sistemas. A prefeitura não informou se houve acesso a dados, e não foi localizada atualização desde então.

Para outros órgãos de saúde: ter um plano de contingência manual já treinado, como o usado nas UPAs, e backups isolados que permitam devolver o sistema ao ar com rapidez.

Fonte: Olhar Direto, 03/11

Atualizações

CASOS DE EDIÇÕES ANTERIORES QUE MUDARAM

TJMG confirma vazamento de arquivos. Em nota de 14/11, o tribunal confirmou que alguns arquivos vazaram, sem dizer quais nem quantas pessoas foram atingidas. Diz que sistemas e bancos de dados seguem íntegros, trocou as senhas de contas em risco, avisou a ANPD e a polícia e está contatando os titulares possivelmente afetados.

Fonte: Nota oficial: TJMG (atualização), 14/11

Mercado Bitcoin: Pix volta nesta terça. Saques e depósitos em reais via Pix voltam a partir de 17/11, só para conta do próprio titular e após nova validação cadastral no app. Negociação e transferências de cripto seguem suspensas, sem data.

Fontes: iProUP, 12/11 · Valor Econômico, 13/11

Mundo

OS CASOS MAIS RELEVANTES DO PERÍODO

GLOBAL · ACESSO REMOTO / MSPS

Worm SCKit usa ScreenConnect para invadir clientes de MSPs

Um operador usou o comando Run de painéis ScreenConnect na nuvem para instalar clientes não autorizados e o kit SCKit, com privilégio SYSTEM, em máquinas gerenciadas por MSPs. Segundo a Huntress, foram cerca de 288 hosts em 48 organizações em 11/11 e mais 205 hosts em 41 organizações em 13/11.

A Huntress liga a entrada à extensão RMM+ (versões 1.0.31 e 1.0.32), que aceitava chave em branco quando não configurada, contornando contas e MFA. A ConnectWise desativou cinco extensões de terceiros em mais de 400 ambientes de parceiros.

Para provedores que usam ScreenConnect: revisar o histórico de Run Command, desativar a RMM+, manter técnicos na versão 26.6.5 ou superior, isolar hosts suspeitos, remover a tarefa TrapWatch e a pasta RelayTrap e trocar credenciais e sessões.

Fontes: Huntress, 13/11 · BleepingComputer, 13/11

EUA · IA OFENSIVA

Google vê criminosos usando agentes de IA para transformar patches em exploits

O Google Threat Intelligence Group (GTIG) relatou em 16/11 que atacantes já usam frameworks autônomos com vários agentes de IA para conduzir intrusões em etapas, indo além do uso manual de chatbots. Entre as ferramentas citadas estão ARTEX, CAIRN, CyberStrikeAI e PentAGI.

Os modelos de linguagem são usados para comparar versões de software e analisar correções recém-publicadas, encurtando o tempo entre o patch e a exploração ativa; o relatório cita o caso de falhas do PaperCut NG/MF exploradas em setembro. Também descreve revenda de acesso a LLMs roubados de empresas (LLMjacking) e um serviço chinês de phishing com chatbot embutido.

Na prática, a janela para aplicar correções críticas em equipamentos expostos ficou menor. O relatório não traz número de vítimas.

Fontes: Nota oficial: Google Threat Intelligence Group, 16/11 · The Hacker News, 16/11

EUA/EUROPA · OPERAÇÃO POLICIAL

Operação TorNado prende 354 em mercados da dark web

DOJ e Europol anunciaram 354 prisões de vendedores e compradores ligados a mercados da dark web já derrubados; os EUA lideram com 132, seguidos de Reino Unido, Hungria, Alemanha e França.

Foram apreendidas cerca de 950 kg de drogas na Europa e 4,8 toneladas nos EUA. A cobertura não cita participação do Brasil.

Fontes: Just The News, 12/11 · Nota oficial: Europol, 12/11

⚠ Alerta: falhas exploradas agora

PRIORIDADE PARA BORDA E FERRAMENTAS DE GESTÃO

Vates Xen Orchestra e XO Appliance (gestão de virtualização XCP-ng)

Sem CVE · aviso Vates VSA-2026-062 (crítico) · fora do KEV da CISA

A Vates publicou em 10/11 o aviso VSA-2026-062, de severidade crítica: um token de login vazio permite contornar a autenticação do Xen Orchestra, console que administra servidores virtuais XCP-ng, e obter acesso de administrador. O fabricante confirma exploração ativa a partir de um IP e de um endereço na rede Tor.

Afeta versões anteriores à 6.9.2 (canal stable) e à 6.10.1 (canal latest), além do XO Appliance. Segundo o The Hacker News, não está claro desde quando a falha é explorada, e um segundo aviso (VSA-2026-063, ligado à importação de VMs) ainda está sem correção.

O QUE FAZER

1. Atualizar para Xen Orchestra 6.9.2 (stable) ou 6.10.1 (latest), com xo-server 5.211.2 ou 5.213.1.
2. Tirar o console da internet e mantê-lo em rede de gestão dedicada; bloquear o IP do aviso e o tráfego Tor.
3. No WAF ou proxy reverso, bloquear requisições com authenticationToken=j:{} (e a forma codificada).
4. Com indício de invasão: trocar todas as senhas e segredos e considerar reinstalar.

Fontes: Nota oficial: Vates (aviso VSA-2026-062), 10/11 · The Hacker News

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.