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 8

Radar de Ciberataques

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

Segunda-feira, 23 de novembro de 2026 Janela: sex 20/11, 07h05 a seg 23/11, 06h57 · inclui o fim de semana Edição nº 8

2	1	3
CASOS NO BRASIL	CONFIRMADOS	FALHAS EXPLORADAS

BRASIL · SETOR PÚBLICO

Governo de Alagoas prepara novo portal após acesso indevido com credencial de administrador

Segundo o Itec, o conteúdo apagado será recuperado de backup e a nova versão do site estava prevista para esta segunda (23/11). O caso reforça a importância da autenticação em dois fatores e da revisão de contas administrativas em portais públicos.

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.

GOVERNO ESTADUAL · AL / MACEIÓ

Acesso com credencial de administrador tira do ar o portal do Governo de Alagoas

CONFIRMADO EM ANDAMENTO Governo do Estado de Alagoas (portal institucional) · acesso indevido com credencial de administrador e alteração do site

Na manhã de 20/11, o portal oficial do Governo de Alagoas saiu do ar após um acesso indevido. Segundo o Itec, órgão de tecnologia do estado, o invasor usou uma credencial válida de administrador a partir da noite de 19/11, alterou a página inicial e apagou notícias, eventos e galerias; apenas o portal foi atingido.

O conteúdo será recuperado de backup e o servidor afetado foi desligado. O Itec previa entregar uma nova versão do portal, no mesmo endereço, nesta segunda (23/11); a Secretaria da Segurança Pública investiga o caso.

Lição para outros órgãos: exigir autenticação em dois fatores nos painéis administrativos de sites, revisar e desativar contas de administrador sem uso e manter backup testado do conteúdo publicado.

Fontes: Estadão Alagoas, 20/11 · Frances News (CadaMinuto), 21/11 · CadaMinuto, 22/11 · Tribuna do Sertão, 22/11

PREFEITURA · MA / SÃO JOÃO DOS PATOS

Polícia apura desvio de recursos da saúde de São João dos Patos (MA)

EM APURAÇÃO EM ANDAMENTO Prefeitura de São João dos Patos (Fundo Municipal de Saúde) · desvio de recursos via sistema de pagamentos; suspeita de engenharia social

A Polícia Civil do Maranhão investiga um acesso indevido ao sistema de pagamentos da Prefeitura de São João dos Patos que desviou recursos do Fundo Municipal de Saúde. Segundo a polícia, em entrevista à Mirante News em 13/11, a estimativa inicial é de cerca de R$ 1 milhão, valor ainda em apuração.

A suspeita inicial é de engenharia social. Lição para outros municípios: dupla aprovação para transferências, limites e alertas no internet banking das contas públicas e confirmação de pedidos por um canal próprio.

Fonte: Blog João Costa (reproduz entrevista à Mirante News), 14/11

FABRICANTE · FIREWALLS SEM SUPORTE

SonicWall pede troca imediata dos firewalls Gen 6, que não terão mais correções

A SonicWall avisou que os firewalls de Geração 6 (SonicOS 6.x) não recebem mais correções de segurança, nem para falhas críticas, e pediu que sejam aposentados e retirados da borda da internet, citando atacantes que usam automação e IA para achar equipamentos sem suporte.

Afeta as linhas TZ300 a TZ600, SOHO/SOHO 250, NSA 2600–6600, NSa 2650–9650, SuperMassive 9200–9800, NSsp 12400/12800 e NSv virtuais. Recomendação: migrar para Gen 8 (SonicOS 8); até lá, desligar gerência pela WAN, restringir ou desligar SSL VPN, exigir MFA, trocar senhas locais e monitorar logs.

Fontes: Nota oficial: SonicWall — Product Advisory: Retire Unsupported Gen 6 Firewalls, 20/11 · The Hacker News, 20/11

Atualizações

CASOS DE EDIÇÕES ANTERIORES QUE MUDARAM

Prefeitura de BH: bancos devolvem o Pix desviado das guias adulteradas. Em nota oficial atualizada em 19/11, a PBH informou cerca de 250 contribuintes afetados entre 14 e 16/11; os valores foram bloqueados e os bancos fazem a devolução automática desde 17/11. Encargos pagos a mais viram crédito tributário.

Fontes: Nota oficial: Prefeitura de Belo Horizonte — nota oficial (atualizada em 19/11), 19/11 · NC News, 20/11

VMware vCenter: CISA confirma exploração. A CVE-2026-123890 entrou no catálogo KEV em 20/11, com prazo de 23/11 para órgãos federais dos EUA e triagem forense exigida. Não há paliativo: é preciso atualizar.

Fonte: Nota oficial: CISA — catálogo KEV, 20/11

Apache Roller: falha também entra no KEV. A CISA incluiu a CVE-2026-129448 no catálogo de falhas exploradas em 20/11, com prazo de 23/11. Correção: Roller 6.1.6 ou superior.

Fonte: Nota oficial: CISA — catálogo KEV, 20/11

Nvidia investiga possível incidente em parceiro. À SecurityWeek, a empresa disse que o caso pode ter atingido um parceiro terceirizado, não nomeado, e que não viu sinal de comprometimento dos próprios sistemas. O grupo que a listou não publicou amostra de dados.

Fonte: SecurityWeek, 19/11

NSA: governo descarta ataque na pane da rede interna. A agência disse operar quase normalmente desde 20/11; o diretor de Inteligência Nacional atribuiu a pane a uma manutenção, e não a ciberataque. Caso encerrado.

Fonte: The Record, 20/11

Mundo

OS CASOS MAIS RELEVANTES DO PERÍODO

CANADÁ · TELECOM

Bell Canada confirma roubo de dados de clientes corporativos por invasor com uso de IA

A Bell Canada, maior operadora do Canadá, avisou clientes corporativos de que um invasor, descrito pela empresa como agente automatizado com IA, roubou dados em 17/11. O incidente foi contido após a descoberta e, segundo a Bell, os serviços aos clientes não foram afetados.

Foram expostos contatos corporativos (nomes, cargos, e-mails, telefones e endereços comerciais), títulos de chamados de suporte, alguns endereços IP ligados a elementos de rede e informações de contexto. A Bell diz que não saíram credenciais, dados pessoais sensíveis nem anexos; não informou quantos clientes foram atingidos nem quem atacou.

Segundo a notificação aos clientes, o alvo foi um ambiente de pré-produção (testes) do sistema Maximo, usado em pedidos e provisionamento de circuitos. A Bell diz que compartilha indicadores técnicos com os clientes e com o Centro Canadense de Segurança Cibernética.

Fontes: BleepingComputer, 20/11 · NetNewsLedger, 22/11

EUA · FORNECEDOR DE DNS/REDE

Infoblox confirma acesso indevido a dados da empresa via fornecedor de migração

A Infoblox, fornecedora de DNS, DHCP e gestão de endereços IP usada por governos, operadoras e grandes empresas, confirmou acesso não autorizado a informações da empresa por meio de um fornecedor terceirizado de migração de dados que tinha acesso ao SharePoint dela. Segundo fontes do The Register, os invasores usaram as contas desse fornecedor para extrair dados.

Do lado dos clientes, foram expostos snapshots de configuração de alguns ambientes NIOS (configurações de DNS e DHCP, bancos de dados do Grid e logs de relatórios). Do lado interno, e-mail do CEO citado pelo The Register aponta dados financeiros e pessoais de funcionários e dependentes.

A empresa diz não ver indício de envolvimento de produtos, serviços em nuvem, atualizações ou processo de build, e recusou-se a informar quantos clientes foram afetados. Quem usa NIOS deve revisar com a Infoblox se seu ambiente está entre os expostos e considerar trocar credenciais e chaves presentes nas configurações.

Fontes: TechCrunch, 16/11 · The Register, 16/11 · TechRadar, 17/11

EUA · POLÍCIA FEDERAL

FBI investiga suspeita de invasão ao banco nacional de dados criminais (NCIC)

A CNN informou em 20/11, citando duas pessoas a par da apuração, que o FBI investiga um aparente comprometimento do NCIC, base usada por polícias federais, estaduais e locais para mandados, antecedentes e checagens. A Reuters repercutiu.

Em 21/11, uma fonte confirmou a investigação à AP; o FBI não comentou. Não foram divulgados os dados atingidos, o volume nem a autoria.

Fontes: SRN News (texto da Reuters), 20/11 · SecurityWeek (texto da AP), 21/11

EUA · LEGISLATIVO ESTADUAL

Ciberataque derruba site e sistemas do Legislativo da Virgínia Ocidental

Um ciberataque iniciado na quinta (19/11) tirou do ar o site do Legislativo da Virgínia Ocidental e afetou seus sistemas de TI; o incidente seguia em curso na sexta, segundo The Record.

A vice-chefe de gabinete da Câmara estadual disse que o incidente foi contido, que o acesso a parte dos sistemas foi desligado temporariamente e que, pelo que se sabe, outros órgãos do estado não foram atingidos. Não disse se foi ransomware; nenhum grupo reivindicou até sexta.

Fonte: The Record (Recorded Future News), 20/11

FRANÇA · CORREIOS / VAZAMENTO

Filial dos Correios franceses tem dados de 22 milhões de pessoas roubados

O grupo La Poste anunciou em 14/11 que a Maileva, que envia correspondências para empresas e órgãos públicos, sofreu em setembro uma invasão com roubo de dados de cerca de 22 milhões de destinatários: nome, sobrenome e endereço postal, além de cartas de cobrança com número de fatura, datas de atendimento e valores.

A empresa diz que dados bancários não foram afetados, notificou a CNIL e registrou queixa; o Ministério Público de Paris abriu investigação. Nenhum grupo reivindicou o ataque até 16/11.

Fontes: Folha de Pernambuco, 16/11 · Siècle Digital (cita comunicado do La Poste), 16/11

⚠ Alerta: falhas exploradas agora

PRIORIDADE PARA BORDA E FERRAMENTAS DE GESTÃO

Cisco Expressway-C e Expressway-E X15.5.3 e anteriores, em cluster (X14 e anteriores sem correção)

CVE-2026-76466 (CVSS 9,8) — advisory cisco-sa-vcs-static-cred-hr7EWZ8t de 21/10/2026; no KEV da CISA desde 20/11, prazo 23/11

A Cisco publicou em 21/10 a correção de uma falha crítica (CVE-2026-76466, CVSS 9,8) no Expressway em cluster, que permite a um atacante remoto sem login executar comandos como root.

Segundo a empresa russa de segurança F6, noticiado em 18/11, criminosos exploraram a falha depois que um exploit público saiu: invadiram dois Expressway expostos à internet de uma empresa na Rússia, chegaram a nós internos do cluster e roubaram credenciais, inclusive de repositórios GitLab.

Em 20/11 a CISA incluiu a falha no catálogo KEV, confirmando exploração ativa, com prazo de 23/11 para órgãos federais dos EUA e exigência de triagem forense. Expressway-E é equipamento de borda comum em órgãos e empresas que usam videoconferência e telefonia Cisco.

O QUE FAZER

1. Atualizar todos os nós do cluster para Expressway X15.5.20 (também corrige a série de hardening de outubro, CVE-2026-76490 a 76497). A Cisco diz que não há workaround.
2. Quem está em X14 ou anterior: migrar para a linha X15, que tem correção.
3. Até atualizar: limitar as portas TCP 4371 e 4372 apenas aos IPs dos nós do cluster (recomendação da F6, não da Cisco).
4. Antes de atualizar, procurar sinais de invasão nos logs de todos os nós, como a entrada nodeup 'wombat@127.0.0.1' no erlang.log apontada pela F6.

Fontes: Nota oficial: Cisco — advisory cisco-sa-vcs-static-cred-hr7EWZ8t, 21/10 · CNews (relato da F6 sobre exploração), 18/11 · Rescana (resumo do advisory e da exploração), 20/11 · Nota oficial: CISA — catálogo KEV (inclusão de CVE-2026-76466 em 20/11, prazo 23/11), 20/11 · SecurityWeek, 20/11

Microsoft Entra Connect Health

sem CVE divulgado; correção no servidor em 19/11/2026

Uma falha na API do Entra Connect Health, serviço que monitora a infraestrutura de identidade local ligada ao Entra (base de login do Microsoft 365), foi explorada para ler metadados de tenants. Segundo a notificação da Microsoft a administradores, a falha existia desde 23/07 e foi descoberta em 9/11.

Foram expostos e-mails de contatos técnicos e administradores, nomes e IDs de tenant, domínios, tipo de licença e status de sincronização; a Microsoft diz que senhas, hashes, tokens e chaves válidas não foram expostos e que não viu mudança de configuração. A correção foi aplicada no servidor em 19/11, sem ação do cliente.

O QUE FAZER

1. Verificar no Azure Service Health / centro de administração se o tenant recebeu a notificação.
2. Avisar a equipe sobre phishing direcionado aos e-mails de administradores e contatos técnicos expostos.
3. Exigir MFA resistente a phishing nas contas privilegiadas.
4. Revisar configurações do Connect Health e os logs de auditoria e de login do Entra.

Fonte: BleepingComputer, 21/11

SAP NetWeaver Enterprise Portal 7.50 (EP-BASIS 7.50, EP-RUNTIME 7.50)

CVE-2025-42884 (CVSS 6,5) — SAP Note 3660969; no KEV da CISA desde 20/11, prazo 23/11

A CISA incluiu em 20/11 no catálogo KEV a CVE-2025-42884, falha de injeção JNDI no SAP NetWeaver Enterprise Portal 7.50 que permite a um atacante sem login ler ou alterar informações do servidor. A SAP corrigiu o problema no Patch Day de novembro de 2025 (nota 3660969).

O CVSS é 6,5 (médio), mas a inclusão no catálogo indica exploração ativa; alvos e autores não foram divulgados.

O QUE FAZER

1. Aplicar a SAP Security Note 3660969 (Patch Day de novembro de 2025) em todo NetWeaver Enterprise Portal 7.50.
2. Se não puder já: restringir o acesso ao Portal a redes confiáveis e bloquear saída do servidor para provedores JNDI/LDAP/RMI externos.
3. Revisar logs do Portal por requisições com propriedades JNDI ou URLs de lookup incomuns.

Fontes: Nota oficial: CISA — catálogo KEV (inclusão de CVE-2025-42884 em 20/11, prazo 23/11), 20/11 · Nota oficial: SAP — boletim de Security Notes 2025 (nota 3660969, nov/2025), 11/11 · CVEFeed (resumo da CVE e registro no KEV), 20/11

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 e Ciberataques por e-mail ou no canal do WhatsApp. É grátis, e você cancela quando quiser.
Inscreva-se: hubterritory.com/radar/inscricao