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 9

Radar de Ciberataques

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

Terça-feira, 24 de novembro de 2026 Janela: seg 23/11, 07h05 a ter 24/11, 06h57 Edição nº 9

0	0	3
CASOS NO BRASIL	CONFIRMADOS	FALHAS EXPLORADAS

MUNDO · SEGURANÇA DE E-MAIL

N-able restabelece painel do Mail Assure e corrige falha usada em ataques

A CISA incluiu a falha (CVE-2026-134624) no catálogo de vulnerabilidades exploradas, com prazo até 26/11 para os órgãos federais dos EUA. Para quem usa o serviço, o passo é recriar as credenciais de API revogadas e revisar os acessos desde 16/11. No Brasil, não houve novo incidente confirmado na janela.

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.

Nenhum incidente novo no Brasil na janela.

Atualizações

CASOS DE EDIÇÕES ANTERIORES QUE MUDARAM

N-able: painel e APIs do Mail Assure voltaram ao ar Segundo a atualização de 22/11, o painel e as APIs voltaram na noite de 21/11; a empresa revogou os tokens de API e OAuth dos clientes e contratou perícia externa, com laudo de causa raiz previsto para até duas semanas. A falha SSRF achada na investigação já foi corrigida na nuvem; a N-able não disse se ela foi a porta de entrada.

Fonte: The Hacker News, 23/11

Mundo

OS CASOS MAIS RELEVANTES DO PERÍODO

EUA · NUVEM / KUBERNETES

Invasão na Rackspace Spot expõe segredos Kubernetes de clientes

A Rackspace avisou clientes que, em 17/11, um terceiro usou credenciais vazadas para entrar em partes da Spot, seu serviço gerenciado de Kubernetes. Com isso podia criar pods, ler Secrets dos clusters afetados e tokens de API e de atualização da plataforma.

A empresa soube do caso em 18/11 por denúncia de um cliente, revogou tokens e sessões, removeu pods indevidos e rotacionou chaves; o console da Spot ficou fora por dias e só voltou por completo em 21/11. Não disse quantos clientes foram atingidos nem se houve roubo de dados.

Orientação aos afetados: reemitir tokens da Spot, baixar novos kubeconfig, trocar todas as credenciais guardadas em Secrets e revisar logs desde 17/11. IoC divulgado: faixa 23.224.0.0/15.

Fontes: BleepingComputer, 21/11 · SC World, 22/11

CHINA · ESPIONAGEM / VPN

Grupo ligado à China usa VPN SoftEther adulterada para espionar governos, diz a Rapid7

A Rapid7 atribui ao Webworm, com confiança moderada, uma versão recompilada do SoftEther VPN Bridge disfarçada de software de monitoramento de rede para manter acesso remoto escondido.

Não há malware novo: o grupo só mudou nomes, caminhos HTTP e configuração cifrada para fugir da detecção. Os alvos citados são governos, provedores de TI e empresas de energia; não há menção ao Brasil.

Para outros órgãos, a prevenção passa por manter inventário do software de VPN e acesso remoto instalado nos servidores e investigar executáveis com nome de ferramenta legítima fora do padrão.

Fontes: Rapid7 — relatório, 23/11 · The Hacker News, 23/11

ÍNDIA · BANCOS / ATAQUES COM IA

Índia alerta para ataques com IA que geraram pagamentos indevidos em bancos

O CERT-In confirmou alerta sobre transações não autorizadas em instituições financeiras e provedores de tecnologia de pagamentos, com uso de agentes de IA; os invasores alteraram cadastros e cadeias de aprovação e usaram os próprios processos legítimos de pagamento.

O I4C fala em perdas de vários crores (sem total oficial), com dinheiro desviado para contas laranja. O CERT-In associa ataques recentes ao grupo Crafty Falcon, sem atribuir este caso.

Fontes: Nota oficial: CERT-In — aviso CIAD-2026-0062, 23/11 · Nota oficial: I4C — advisory a bancos e NBFCs, 23/11 · The Hacker News, 23/11

GLOBAL · PAGAMENTOS / E-COMMERCE

Cleverbridge confirma roubo de números de cartão e CVV de clientes

A Cleverbridge, plataforma que processa compras e assinaturas para fabricantes de software (o site lista clientes como Red Hat, Sony,

SUSE, Veeam, Tenable e Jamf), detectou atividade não autorizada em 4/11 e começou a notificar os afetados em 20/11.

Segundo o aviso aos clientes, foram copiados número do cartão, validade e código CVV/CVC, e potencialmente e-mail, endereço de cobrança e telefone; senhas não foram afetadas. A empresa diz que não houve criptografia de sistemas e não informou como os invasores entraram nem quantas pessoas foram atingidas.

A Cleverbridge diz ter avisado autoridades de proteção de dados, bandeiras de cartão e polícia, e oferece 24 meses de monitoramento de crédito.

Fontes: Help Net Security, 23/11 · The Register, 23/11 · Nota oficial: Cleverbridge — atualização do incidente, 20/11

EUA · PORTOS

Portos dos EUA relatam milhares de tentativas de invasão por dia

Reportagem de 23/11 (Anadolu, com dados do Financial Times) diz que portos e navios dos EUA enfrentam alta de ciberataques. O Porto de Corpus Christi (TX), maior exportador de petróleo do país, relata centenas e às vezes milhares de tentativas de invasão por dia, segundo seus executivos.

A autoridade portuária de NY/NJ diz investir em defesa em camadas; Oakland não comentou. Especialistas citados apontam operações ligadas a Irã, Coreia do Norte e China contra o transporte marítimo. A matéria não relata incidente com dano.

Fonte: The Express Tribune / Anadolu, 23/11

⚠ Alerta: falhas exploradas agora

PRIORIDADE PARA BORDA E FERRAMENTAS DE GESTÃO

N-able Mail Assure (SpamExperts)

CVE-2026-134624 — prazo da CISA: 2026-11-26

A CISA incluiu em 23/11 no catálogo de falhas exploradas uma SSRF no N-able Mail Assure (SpamExperts): a checagem de conexão da sincronização LDAP deixa um usuário autenticado da API, com acesso de alto nível, alcançar hosts e portas internos e enviar dados forjados a serviços internos.

A N-able diz que achou a falha durante a investigação da invasão a um servidor da nuvem do Mail Assure (ver item mundo-2026-11-n-able-mail-assure) e que a corrigiu na versão 20261121.1943; não afirmou que ela foi a porta de entrada. A CISA pede triagem forense e, para serviço em nuvem, seguir as orientações do fabricante ou deixar de usar o produto.

O QUE FAZER

1. Na nuvem (Hosted Cloud) a N-able já corrigiu; no SpamExperts Local Cloud, confirmar que o servidor está na versão 20261121.1943 ou superior.
2. Recriar as credenciais de scripts e integrações: a N-able revogou os tokens de API e OAuth dos clientes.
3. Revisar usuários de API ativos, a configuração de sincronização LDAP e os logs de acesso da API a partir de 16/11.
4. Quem é MSP e não recebeu o e-mail de orientação da N-able deve acionar o suporte.

Fontes: Nota oficial: CISA — catálogo KEV (cópia oficial no GitHub), 23/11 · Nota oficial: N-able — boletim de segurança (citado pelo KEV; página não carregou), 23/11 · The Hacker News, 23/11

ConnectWise ScreenConnect (cliente host do técnico)

CVE-2026-84869 (CVSS 9,9) — no KEV da CISA desde 11/09/2026; prazo da CISA: 14/09/2026

Uma campanha distinta da onda SCKit explora a CVE-2026-84869: um 'convidado' numa sessão remota envia e executa um arquivo na máquina do técnico que se conecta. Num caso de 12/11, um .bat roubou dados via Telegram e instalou um ScreenConnect malicioso ligado ao relay do atacante em cerca de 9 segundos.

Segundo a Huntress, de 20/10 a 16/11 houve ao menos 688 mil pedidos de execução de arquivos update.bat, de 29 IPs contra 42 servidores; outro grupo usou sessões falsas com nomes de corretoras de cripto em 118 servidores de 109 organizações.

Para provedores e equipes de TI: atualizar o cliente dos técnicos para 26.6.5 ou superior; sem isso, retirar a permissão TransferFiles das funções de sessão.

O QUE FAZER

1. Atualizar o cliente host do ScreenConnect dos técnicos para a versão 26.6.5 ou superior (boletim ConnectWise de 08/09/2026).
2. Se não der para corrigir já, remover a permissão TransferFiles de funções e grupos de sessão.
3. Procurar arquivos update.bat / update_<hex>.bat e clientes ScreenConnect desconhecidos nas estações dos técnicos.
4. Isolar estações afetadas e trocar credenciais acessíveis a partir delas.

Fontes: Nota oficial: CISA KEV (catálogo oficial no GitHub), 11/09 · Nota oficial: ConnectWise — boletim de segurança ScreenConnect, 08/09 · The Hacker News, 23/11

Idunno.AntiCsrf (módulo anti-CSRF para ASP.NET WebForms) 0.9.1.0 e 0.9.1 Beta

CVE-2026-131914 (CVSS 9.3; fora do KEV até 24/11)

A Mandiant (Google) divulgou falha crítica de desserialização na biblioteca Idunno.AntiCsrf, usada em sites ASP.NET WebForms; um único POST HTTP sem login basta para executar código no servidor.

A Mandiant diz ter observado exploração ativa, sem dar detalhes de quem ataca. O projeto está abandonado desde 2008 e não haverá correção.

O QUE FAZER

1. Procurar Idunno.AntiCsrf.dll nas pastas bin/ e referências no Web.config dos sites ASP.NET WebForms, inclusive sistemas legados.
2. Não há correção: remover a biblioteca (abandonada desde 2008) e trocar por AntiForgery do System.Web.Helpers, ViewStateUserKey com ViewState protegido ou IAntiforgery do ASP.NET Core.
3. Revisar logs do IIS atrás de POSTs anômalos a páginas .aspx com retorno 302 ou 500.
4. Se houver sinal de invasão: trocar machineKey, chaves de criptografia e senhas de banco, e inspecionar o webroot atrás de arquivos estranhos.

Fontes: Nota oficial: Mandiant — boletim MNDT-2026-0048, 23/11 · The Hacker News, 23/11

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