Your IT Company

Principais Vulnerabilidades e Ameaças (abril/26)

Sumário

1. Objetivo

Este documento foi desenvolvido e fundamentado nas documentações oficiais do NIST (National Institute Of Standards and Technology), MITRE e CVE.org, que são mundialmente conhecidas na área de cibersegurança como modelos de padronização das melhores práticas de segurança, pesquisa de metodologias de ataques, defesa cibernética e catalogação de novas vulnerabilidades em sistemas operacionais e aplicações.

2. Vulnerabilidades e Ameaças descobertas

2.1. Microsoft Exchange e driver CLFS do Windows: vulnerabilidades exploradas ativamente

A CISA adicionou duas vulnerabilidades críticas ao seu catálogo KEV: uma falha de RCE no Microsoft Exchange Server (CVE-2023-21529) e uma leitura fora dos limites no driver Windows CLFS que permite elevação de privilégio local (CVE-2023-36424). A agência alerta que ambas estão sendo exploradas ativamente e exige correção imediata por agências federais, com forte recomendação para o setor privado aplicar patches urgentemente.

Exploração

A CVE-2023-21529 afeta o **Microsoft Exchange Server** e tem origem em desserialização de dados não confiáveis. Um atacante autenticado pode manipular o processamento interno de dados para executar código remoto no servidor. Com isso, é possível obter acesso persistente, movimentar-se lateralmente na rede e explorar o ambiente corporativo, especialmente porque servidores Exchange armazenam comunicações sensíveis e frequentemente servem como ponto de entrada estratégico.

A CVE-2023-36424 impacta o **Windows Common Log File System**, sendo uma falha de leitura fora dos limites. Esse tipo de vulnerabilidade permite que um atacante com acesso local escale privilégios até nível administrativo. Em ataques reais, ela costuma ser utilizada após o acesso inicial, permitindo desativar mecanismos de segurança e facilitar a implantação de ransomware ou backdoors.

Do ponto de vista operacional, ambas as falhas foram incluídas no catálogo KEV da Cybersecurity and Infrastructure Security Agency em 13 de abril de 2026. A diretiva BOD 22-01 estabelece prazo até 27 de abril de 2026 para aplicação das correções em ambientes federais, e a confirmação de exploração ativa eleva significativamente a criticidade e urgência de mitigação.

Mitigação e Prevenção

- **Ações imediatas recomendadas:**
  - Aplicar patches oficialmente publicados pela Microsoft para Exchange Server e para o Windows (incluindo correções do driver CLFS) imediatamente.
  - Cumprir o prazo e orientações do BOD 22-01 se for uma entidade federal; organizações privadas devem priorizar igual urgência.
- **Se não for possível aplicar o patch imediatamente:**
  - Isolar sistemas vulneráveis (segmentação de rede, regras de firewall restringindo acesso ao Exchange).

- Descontinuar o uso do produto vulnerável ou mover serviços para ambientes não afetados até correção.

- **Para administradores de Exchange:**
  - Revisar e reforçar controles de autenticação (MFA para contas administrativas e acesso remoto).
  - Restringir exposição de serviços Exchange à internet; usar proxys/reverse proxies com WAF quando necessário.
  - **Monitorar logs do Exchange e SIEM para sinais de RCE:** processos incomuns, shells reversos, criação de contas administrativas inesperadas, tarefas agendadas novas.
  - Aplicar princípios de menor privilégio e revisar contas com privilégios elevados.
- **Operações de segurança e resposta a incidentes:**
  - Garantir atualizações de segurança do Windows e mitigação de exploit mitigations (Windows Exploit Protection / DEP / ASLR).
  - Limitar contas com direitos locais de administrador; usar contas separadas para administração.
  - Habilitar EDR/antivírus com regras comportamentais para detectar tentativas de escalonamento de privilégio e manipulação de drivers.
- **Operações de segurança e resposta a incidentes:**
  - Executar varreduras forenses em servidores Exchange e hosts Windows sensíveis para identificar atividade suspeita.
  - Preparar playbooks de resposta (isolar host, recolher logs, reverter privilégios, aplicar remediação).
  - Comunicar às equipes de TI e negócios sobre risco e janelas de manutenção para aplicação de patches.
- **Para provedores de serviços em nuvem/terceirizados:**
  - Verificar se seus provedores aplicaram correções e seguem orientação BOD 22-01 quando aplicável.
  - Exigir evidência de correção ou mitigação para sistemas gerenciados.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/microsoft-exchange-and-windows-clfs-vulnerabilities-exploited/.

2.2. CVE-2026-2262: Easy Appointments (WordPress) expõe dados sensíveis via REST API

O Easy Appointments (plugin WordPress) vem permitindo acesso não autenticado ao endpoint REST /wp-json/wp/v2/eablocks/ea_appointments/ e expondo dados sensíveis de agendamentos (nomes, e-mails, telefones, IPs, descrições e preços). A falha afeta todas as versões até 3.12.21 e representa risco imediato de vazamento de dados de clientes e uso malicioso para phishing, fraude ou violação de privacidade.

Exploração

A falha ocorre porque o endpoint foi registrado sem qualquer verificação de autenticação ou autorização, utilizando permission_callback => '__return_true'. Isso permite que qualquer requisição GET acesse e retorne dados de agendamentos sem restrição.

O principal alvo são sites que utilizam o plugin **Easy Appointments** no **WordPress**, expondo informações de clientes e visitantes que realizaram agendamentos.

O impacto inclui vazamento de dados pessoais, como informações de contato e horários, o que pode ser explorado em campanhas de engenharia social ou phishing. Além disso, há risco de não conformidade com regulamentações como a **Lei Geral de Proteção de Dados**, podendo resultar em danos reputacionais e implicações legais para os responsáveis pelo site.

Mitigação e Prevenção

- **Ações imediatas:**
  - **Atualização:** atualizar o plugin Easy Appointments para a versão corrigida (ou superior a 3.12.21, verificar se 3.12.22 ou posterior está disponível) assim que possível.
  - **Bloqueio do endpoint:** se não for possível atualizar imediatamente, bloquear o acesso público ao endpoint /wp-json/wp/v2/eablocks/ea_appointments/ via WAF, regras do servidor (nginx/Apache) ou .htaccess. Exemplo (nginx): **location ~ ^/wp-json/wp/v2/eablocks/ { deny all; }**
  - **Remoção temporária:** desativar/remover o plugin Easy Appointments até que a atualização seja aplicada.
  - **Correção do código (para administradores que mantêm o site):** alterar o registro da rota REST para usar um permission_callback que valide autenticação/autorização adequada (por exemplo, current_user_can('manage_options') ou callback personalizado). Alternativamente, remover o endpoint via filtro rest_endpoints. Testar em ambiente não-prod antes de aplicar.
  - **Auditoria e detecção:** revisar logs de acesso (webserver e logs do WP REST API) procurando requisições ao endpoint afetado; identificar possíveis extrações de dados e janelas de exposição.

- **Resposta a incidentes:** se houver indícios de acesso não autorizado, considerar notificar usuários afetados, seguir obrigações legais/regulatórias (LGPD) e recolher evidências.
- **Defesa em profundidade:** restringir exposição de APIs privadas, aplicar princípio do menor privilégio, manter plugins e WP sempre atualizados, usar WAF e monitoramento contínuo.
- **Para usuários finais:** se você é cliente de um site afetado, peça confirmação ao administrador sobre exposição de seus dados; monitore comunicações suspeitas e altere credenciais se necessário.

IOCs

- **Endpoint REST afetado:** /wp-json/wp/v2/eablocks/ea_appointments/
- **Caminho do arquivo do plugin:** wp-content/plugins/easy-appointments/ea-blocks/ea-blocks.php
- **Plugin (slug):** easy-appointments
- **Versões afetadas:** todas até e incluindo 3.12.21

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://www.tenable.com/cve/CVE-2026-2262, https://www.wordfence.com/threat-intel/vulnerabilities/id/e681aa8e-522e-4092-aa1f-8ada3097c8d6?source=cve..

2.3. PoC público para vulnerabilidade crítica no FortiSandbox permite RCE como root

Um PoC (proof-of-concept) foi publicado para uma falha crítica no Fortinet FortiSandbox que permite execução remota de comandos do sistema operacional com privilégios *root* sem autenticação. A vulnerabilidade, explorável via parâmetro GET, afeta FortiSandbox 4.4.0 a 4.4.8 e deve ser corrigida imediatamente devido à disponibilidade pública do exploit.

Exploração

A vulnerabilidade é uma injeção de comandos no sistema operacional que permite execução de comandos como root sem necessidade de autenticação no **FortiSandbox**. O problema está no endpoint /fortisandbox/job-detail/tracer-behavior, onde o parâmetro jid não é devidamente sanitizado. Isso permite que um atacante injete comandos utilizando caracteres como |, comuns em sistemas Unix para encadeamento de instruções.

Na prática, um invasor pode enviar uma simples requisição HTTP manipulada e executar comandos remotamente no sistema. Isso possibilita, por exemplo, gravar a saída de comandos em arquivos acessíveis via web, facilitando o controle e a exploração contínua do ambiente. As versões afetadas vão de 4.4.0 até 4.4.8.

O impacto é crítico, incluindo leitura de arquivos sensíveis, escrita de arquivos na web root, implantação de malware e comprometimento total do host com privilégios de root, permitindo controle completo do sistema.

Mitigação e Prevenção

- **Ações imediatas:**
  - **Aplique o patch agora:** atualize FortiSandbox para a versão corrigida indicada no advisory oficial (não deixe instâncias em 4.4.0–4.4.8 em produção).
  - **Isolamento:** retirar instâncias afetadas da rede pública até aplicar atualização ou bloqueio adequado.
  - **Restrinja acesso:** permita acesso à interface de gerenciamento apenas de redes e IPs confiáveis (ACLs, VPN).
  - **Regras WAF/IPS:** criar regras para bloquear requisições ao endpoint /fortisandbox/job-detail/tracer-behavior contendo caracteres de pipe (|) ou padrões de injeção em jid.
  - **Verificação de comprometimento:** procurar arquivos recém-criados na web root (ex.: /web/ng/out.txt), modificações inesperadas no sistema, processos/cronjobs suspeitos e conexões de saída incomuns.
  - **Resposta a incidente:** se houver evidência de exploração, isolar o sistema, coletar artefatos e considerar rebuild a partir de backup confiável; assumir comprometimento com privilégios root.
- **Recomendações por público:**
  - **Administradores de sistema:** aplicar patch, revisar exposição do gerenciamento, configurar firewall/WAF/IDS, revisar logs e realizar varredura forense.
  - **Equipes de segurança operacional (SOC):** criar assinaturas/alertas para requisições GET ao endpoint com parâmetros contendo |, e monitorar criação de arquivos na web root.
  - **Usuários finais:** não aplicável diretamente (não interajar com interfaces administrativas expostas); informar equipe de TI caso a organização utilize FortiSandbox.

IOCs

- **Endpoint alvo:** /fortisandbox/job-detail/tracer-behavior
- **Parâmetro de injeção:** jid contendo o caractere pipe | (ex.: jid=|(id > /web/ng/out.txt)|)
- **Exemplo de arquivo criado pelo PoC:** /web/ng/out.txt (indicador de possível exploração)
- **Exemplo de comando PoC (detecção/caça):**
  curl -s -k --get "http://$HOST/fortisandbox/job-detail/tracer-behavior" --data-urlencode "jid=|(id > /web/ng/out.txt)|"

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/poc-exploit-fortisandbox-vulnerability.

2.4. Hackers usam ATHR para executar vishing com IA e roubo de credenciais

ATHR é uma plataforma de crime cibernético que automatiza ataques de vishing (phishing por telefone) usando um agente de voz com IA para enganar vítimas e roubar credenciais em escala. A ameaça é relevante porque emails com apenas um número de telefone contornam filtros tradicionais e permitem ataques coordenados, escaláveis e de baixo custo.

Exploração

O método utilizado é o TOAD, Telephone-Oriented Attack Delivery, em que o ataque acontece por ligação telefônica em vez de links ou anexos. Isso reduz a eficácia de filtros tradicionais de e-mail e aumenta a chance de interação da vítima.

A arquitetura do ATHR é integrada e baseada em navegador, composta por um sistema de envio de e-mails, um agente de voz com IA, identificado como modelo “Sonic 3”, um painel de captura de credenciais em tempo real e um ambiente unificado para operação dos atacantes.

O fluxo do ataque começa com o envio de e-mails contendo apenas um número de telefone. Quando a vítima liga, o agente de IA conduz uma conversa estruturada, simulando suporte técnico, validações de segurança e supostas atividades suspeitas. Durante a interação, a vítima pode ser induzida a fornecer códigos de verificação ou redirecionada para páginas falsas que capturam credenciais em tempo real.

Os principais alvos incluem usuários de serviços amplamente utilizados como **Google**, **Microsoft**, **Yahoo**, **AOL** e plataformas de criptomoedas como **Coinbase**, **Binance**, **Gemini** e **Crypto.com**.

O impacto inclui roubo de credenciais, comprometimento de contas, perdas financeiras e acesso indevido a dados corporativos. A eficácia do ataque está no fato de que os e-mails não contêm links ou anexos maliciosos, podendo passar por validações como SPF, DKIM e DMARC, enquanto a voz sintética convincente aumenta a confiança da vítima e a taxa de sucesso.

Mitigação e Prevenção

- **Recomendações gerais:**
  - **Treinamento de usuário:** instruir colaboradores a NUNCA ligar para números que apareçam em emails inesperados de “alerta de segurança”, sempre verificar a notificação diretamente pelo site oficial ou app da empresa.
  - **Procedimentos de verificação:** estabelecer canais oficiais de suporte e procedimentos de verificação de identidade (códigos internos, validação por outro canal) antes de aceitar qualquer solicitação por telefone.
  - **Política de reset e MFA:** exigir autenticação forte (MFA com tokens físicos ou apps autenticadores) e revisar fluxos de recuperação de conta para reduzir dependência de códigos enviados por SMS/voz.
  - **Monitoramento e detecção:** criar regras no SIEM/EDR/Email Gateway para detectar padrões anômalos, por exemplo: múltiplos destinatários que recebem mensagens

com o mesmo número de telefone em curto espaço de tempo; aumento súbito de emails com corpo contendo somente números de telefone.

- **Filtragem e análise de conteúdo:** configurar gateways de email para sinalizar mensagens que contenham apenas um número de telefone como possível TOAD/vishing e exigir inspeção manual.
- **Proteção baseada em comportamento:** implantar soluções de detecção comportamental (behavioral AI) que mapeiem padrões normais de comunicação e alertem sobre anomalias entre remetente e destinatário.
- **Hardening para equipes de suporte:** treinar equipes internas a confirmar identidades por métodos pré-definidos, registrar chamadas de suporte e adicionar autenticação adicional antes de executar ações sensíveis.
- **Resposta a incidentes:** preparar playbooks específicos para vishing, incluir bloqueio/monitoramento de contas afetadas, reset de senhas, remoção de sessões ativas e investigação de possíveis exfiltrações.
- **Colaboração com telefones/carriers:** reportar números usados em campanhas de vishing para operadoras e listas de bloqueio.

- **Recomendações por público:**
  - **Administradores de sistema / Segurança:** implementar regras SIEM para correlação email→chamada, aplicar políticas de proteção da conta, revisar fluxos de recuperação e implantar solução de detecção comportamental.
  - **Usuários finais / Colaboradores:** não ligar para números em emails suspeitos; confirmar alertas diretamente pelo site ou app oficial; ativar MFA forte; relatar imediatamente tentativas de vishing ao time de segurança.
  - **Equipes de suporte/atendimento:** exigir verificações adicionais para alterações sensíveis e orientar clientes sobre canais oficiais de contato.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/hackers-use-athr-to-run-ai-powered-vishing-credential-theft/.

2.5. CVE-2026-20184: Vulnerabilidade crítica no Cisco Webex Services permite impersonação total via SSO

A Cisco divulgou um advisory sobre uma falha crítica em seus serviços Webex na nuvem que permite a um atacante remoto não autenticado burlar completamente a autenticação e se passar por qualquer usuário. A falha afeta integrações SSO (SAML) no Webex Control Hub e tem CVSS 9.8, ação imediata dos administradores é necessária, pois não há workaround temporário.

Exploração

A vulnerabilidade está relacionada à validação incorreta de certificados na implementação de SSO do **Cisco Webex**, classificada como CWE-295. Esse problema permite que tokens de autenticação não confiáveis sejam aceitos como válidos.

O vetor de ataque consiste em um invasor que se conecta ao endpoint vulnerável e envia um token de autenticação especialmente forjado. Devido à falha na validação, o sistema aceita esse token e concede acesso como se fosse um usuário legítimo.

O principal alvo são organizações que utilizam SSO baseado em SAML integrado ao Webex Control Hub, especialmente ambientes corporativos com uso intensivo da plataforma para reuniões e comunicação interna.

O impacto potencial inclui comprometimento de contas corporativas, acesso a comunicações e arquivos de reuniões, exposição de dados sensíveis e possibilidade de movimentação lateral e elevação de privilégios dentro do ambiente. A vulnerabilidade foi identificada em testes internos da **Cisco** e, até o momento, não há evidências públicas de exploração ativa, mas o risco é considerado alto devido à criticidade da falha.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Leia e siga o advisory oficial da Cisco (cisco-sa-webex-cui-cert-8jSZYhWL).
  - Faça o upload imediato de um *novo certificado SAML* do seu Identity Provider (IdP) diretamente no Webex Control Hub, isso é obrigatório para encerrar a exposição no lado do cliente.
  - Revogue/rotacione o certificado SAML antigo no IdP e no Control Hub para garantir que tokens antigos ou forjados não sejam aceitos.
  - Valide no Control Hub que as configurações de SSO correspondem às recomendações do IdP (assinaturas, issuer, audience, endpoints).
  - Teste a integração SSO em ambiente de homologação antes de aplicar em produção e agende a alteração em janela de manutenção para minimizar impacto.
  - Forçar invalidação de sessões ativas e exigir novos logins após a troca de certificado, quando aplicável.
  - Habilite e revise logs de autenticação SAML no Webex e no IdP; crie alertas para sessões incomuns, tokens com assinaturas inválidas ou autenticações de origens não usuais.
  - Implemente monitoramento via SIEM para detectar picos de autenticação, criação de sessão em massa ou hashes/assuntos de token anômalos.
  - Restrinja privilégios administrativos no Control Hub e aplique controles de acesso baseados em funções.

- Coordene com o suporte do IdP e da Cisco para confirmar que o backend já recebeu a correção e que sua configuração local está em conformidade.

- **Recomendações (Usuários finais / Gestores):**
  - Siga as orientações da equipe de TI da sua organização. Caso tenha recebido orientação para logout/re-login, faça-o.
  - Fique atento a convites de reunião inesperados, mudanças de acesso a arquivos ou comunicações que pareçam fora do padrão e reporte ao time de segurança.
  - Evite reutilizar credenciais em outros serviços e mantenha MFA ativado quando possível (embora o exploit afete o fluxo SSO, MFA ainda ajuda em outros vetores).

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/cisco-webex-services-vulnerability/.

2.6. Criminosos abusam da automação AI n8n para distribuir malware e burlar filtros

O n8n, uma plataforma legítima de automação de workflows, foi usada por atacantes para enviar e-mails de phishing e distribuir cargas maliciosas a partir de subdomínios confiáveis (*.app.n8n.cloud), o que ajuda a contornar filtros tradicionais de segurança. A campanha, observada entre outubro de 2025 e março de 2026, combinou fingerprinting por pixel invisível e entrega de RMMs modificados para obter persistência e exfiltração.

Exploração

O vetor de abuso envolve a criação de contas gratuitas no **n8n**, que geram automaticamente subdomínios sob *.app.n8n.cloud. Esses subdomínios são utilizados para hospedar webhooks expostos, funcionando como canal de entrega de ataques.

O mecanismo consiste no envio de e-mails HTML que incorporam esses webhooks. Eles podem atuar como pixels de rastreamento para coleta de informações ao abrir o e-mail e como páginas que executam JavaScript para forçar o download de arquivos maliciosos, como executáveis ou MSI. Em um cenário observado, a vítima precisava resolver um CAPTCHA antes do download de um arquivo disfarçado, que instalava uma versão modificada do **Datto RMM**. Em outro caso, um instalador MSI implantava uma versão alterada do **ITarian**. Os principais alvos são usuários corporativos que confiam em domínios aparentemente legítimos e endpoints que permitem execução de instaladores.

O impacto inclui instalação de ferramentas de acesso remoto persistente, exfiltração de dados, movimentação lateral na rede e evasão de detecção, já que a infraestrutura utilizada possui reputação legítima.

Mitigação e Prevenção

- **Recomendações gerais:**
  - Implementar detecção comportamental além de bloqueio estático de domínio; monitorar padrões anômalos de tráfego para domínios de plataformas de automação.

- Manter inventário aprovado de fluxos e plataformas de automação (ex.: n8n) e bloquear/alertar comunicações de endpoints que tentem acessar endpoints não aprovados desses serviços.

- **Recomendações para administradores:**
  - Inventariar uso legítimo de n8n e permitir apenas subdomínios/workflows aprovados.
  - Configurar regras de prevenção de perda de dados (DLP) e proxies que inspecionem downloads iniciados por páginas hospedadas em plataformas de terceiros.
  - Monitorar criação e uso de tarefas agendadas, instalação de serviços RMM e execução de PowerShell anômalo; bloquear criação automática de tarefas por binários não assinados.
  - Aplicar lista de bloqueio/alerta para comunicações com domínios suspeitos identificados e para padrões de webhook incomuns.
- **Recomendações para usuários finais:**
  - Desconfiar de e-mails inesperados que simulem notificações de compartilhamento (OneDrive, Google Drive etc.) e não abrir links/arquivos sem verificação.
  - Não executar arquivos .exe ou .msi recebidos por e-mail; confirmar com remetente por canal separado.

IOCs

- **Namespace utilizado:** subdomínios sob *.app.n8n.cloud
- **Nome de arquivo observado:** DownloadedOneDriveDocument.exe
- **Domínio de relay/C2 citado:** centrustage[.]net
- **Padrão de vetor:** URLs de webhooks do n8n com páginas HTML/JS que forçam downloads (estrutura de webhook indicada no artigo, sem URLs completas divulgadas)

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/hackers-abuse-n8n-ai-workflow-automation/.

Esta publicação tem como objetivo orientar a equipe interna e os nossos clientes sobre ameaças emergentes no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

A publicação do documento de Inteligência de Ameaças será realizada quinzenalmente.

Produzido por: Equipe de Threat Intelligence da Service IT Security