Your IT Company

Principais Vulnerabilidades e Ameaças (maio/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. CVE-2026-32202: Microsoft confirma exploração ativa do Windows Shell

A Microsoft confirmou a exploração ativa da vulnerabilidade CVE-2026-32202, uma falha de spoofing presente no Windows Shell. O problema permite que atacantes manipulem arquivos maliciosos para mascarar sua real extensão ou comportamento, fazendo com que o usuário execute conteúdo malicioso acreditando tratar-se de um arquivo legítimo. A vulnerabilidade afeta diferentes versões suportadas do Windows e já vem sendo utilizada em campanhas reais de comprometimento.

Exploração

A exploração normalmente ocorre por meio de campanhas de phishing, anexos maliciosos e downloads hospedados em sites comprometidos. O atacante cria arquivos especialmente manipulados utilizando características do Windows Shell para ocultar extensões reais ou alterar a forma como o arquivo é exibido ao usuário.

Em cenários observados, o usuário recebe documentos compactados ou arquivos aparentemente legítimos, como PDFs, imagens ou documentos Office. Após a execução, o malware:

- Estabelece persistência no sistema;
- Realiza download de payloads secundários;
- Rouba credenciais armazenadas no navegador;
- Coleta informações do sistema;
- Possibilita movimentação lateral na rede;
- Implanta loaders, trojans ou ransomware.

A exploração depende da interação do usuário, porém a simplicidade do ataque aumenta significativamente sua eficácia em campanhas de engenharia social.

Mitigação e Prevenção

- **Ações imediatas recomendadas:**
  - Aplicar imediatamente os patches disponibilizados pela Microsoft;
  - Bloquear arquivos suspeitos recebidos via e-mail;
  - Revisar políticas de execução de arquivos em endpoints;
  - Atualizar assinaturas de antivírus e EDR.
- **Recomendações para Administradores de Sistema:**
  - Habilitar visualização completa de extensões de arquivos no Windows;

- Restringir execução em diretórios temporários e %AppData%;
- Implementar Application Control/AppLocker;
- Monitorar execução suspeita via explorer.exe;
- Habilitar logs avançados de PowerShell e Sysmon;
- Implementar segmentação de rede para limitar movimentação lateral.

- **Recomendações para Usuários Finais:**
  - Não abrir anexos de remetentes desconhecidos;
  - Verificar cuidadosamente extensões de arquivos;
  - Evitar downloads de fontes não confiáveis;
  - Reportar arquivos suspeitos ao time de segurança;
  - Manter sistema operacional e antivírus atualizados.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://thehackernews.com/2026/04/microsoft-confirms-active-exploitation.html.

2.2. CVE-2026-35414: Vulnerabilidade no OpenSSH permite Bypass de autenticação baseada em certificados

A CVE-2026-35414 afeta versões do OpenSSH anteriores à 10.3 e está relacionada ao tratamento inadequado de “principals” durante autenticação baseada em certificados SSH. A vulnerabilidade pode permitir bypass de controles de autenticação em ambientes que utilizam certificados assinados por autoridades certificadoras (CA).

Exploração

A exploração ocorre em ambientes que utilizam autenticação baseada em certificados SSH e configurações específicas envolvendo authorized_keys e principals. Um atacante com acesso a certificados válidos ou parcialmente confiáveis pode manipular parâmetros utilizados na validação de autenticação.

Em ambientes vulneráveis, a falha pode permitir:

- Bypass de restrições de autenticação
- Acesso indevido a servidores Linux
- Escalada de privilégios em ambientes administrativos
- Persistência via inclusão de novas chaves SSH
- Movimentação lateral entre servidores corporativos

Ambientes automatizados, infraestruturas DevOps e servidores expostos à internet apresentam maior risco operacional.

Mitigação e Prevenção

- **Ações imediatas:**
  - Atualizar imediatamente para OpenSSH 10.3 ou superior.
  - Revisar todas as configurações relacionadas a certificados SSH

- Revogar certificados suspeitos ou não utilizados.
- Auditar acessos recentes via SSH

- **Recomendações para Administradores de Sistema:**
  - Restringir autenticação baseada em certificados apenas ao necessário.
  - Implementar MFA para acessos administrativos
  - Limitar acesso SSH por VPN ou allowlist de IPs
  - Monitorar logs /var/log/auth.log e eventos SSH
  - Desabilitar autenticação root remota quando possível
  - Revisar políticas de rotação de chaves e certificados
- **Recomendações para Usuários Finais:**
  - Utilizar apenas chaves autorizadas pela organização
  - Não compartilhar certificados SSH
  - Informar acessos inesperados ou falhas de autenticação
  - Utilizar dispositivos confiáveis para conexões administrativas

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://nvd.nist.gov/vuln/detail/CVE-2026-35414.

2.3. CVE-2026-0300: Vulnerabilidade crítica no Palo Alto PAN-OS permite execução remota de código em Firewalls

A Palo Alto Networks divulgou a CVE-2026-0300, uma vulnerabilidade crítica de buffer overflow presente no serviço User-ID Authentication Portal (Captive Portal) do PAN-OS. A falha permite execução remota de código sem autenticação com privilégios elevados diretamente no firewall. A exploração ativa já foi confirmada pela fabricante.

Exploração

A exploração ocorre através do envio de pacotes especialmente manipulados para o serviço Captive Portal exposto na interface do firewall. A vulnerabilidade permite corrupção de memória e execução arbitrária de código diretamente no PAN-OS. Após comprometimento bem-sucedido, os atacantes podem:

- Executar comandos remotamente
- Implantar persistência no equipamento
- Interceptar tráfego monitorado pelo firewall
- Criar túneis de acesso remoto
- Desabilitar mecanismos de segurança
- Movimentar lateralmente pela rede corporativa
- Apagar logs para dificultar análise forense

Pesquisadores identificaram uso de shellcodes diretamente em processos nginx do PAN-OS durante ataques observados.

Mitigação e Prevenção

- **Ações imediatas:**
  - Aplicar imediatamente os patches disponibilizados pela Palo Alto
  - Desabilitar temporariamente o Captive Portal
  - Restringir exposição do serviço à internet
  - Revisar indicadores de comprometimento no equipamento
- **Recomendações para Administradores de Sistema:**
  - Segmentar interfaces administrativas
  - Restringir gerenciamento apenas a redes confiáveis
  - Implementar MFA para administradores
  - Monitorar logs do PAN-OS e nginx
  - Revisar regras de firewall e acessos remotos
  - Habilitar monitoramento contínuo de integridade
- **Recomendações para Usuários Finais:**
  - Reportar falhas de conectividade incomuns
  - Não utilizar credenciais administrativas fora de ambientes autorizados
  - Alterar senhas caso haja suspeita de comprometimento

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://thehackernews.com//2026/05/palo-alto-networks-firewall-vulnerability.html.

2.4. CVE-2026-23918: Falha crítica no Apache HTTP/2 pode levar a DoS e execução remota de código

A CVE-2026-23918 é uma vulnerabilidade crítica presente no módulo mod_http2 do Apache HTTP Server 2.4.66. A falha está relacionada a um erro de “double free” durante o processamento de streams HTTP/2, podendo causar corrupção de memória, negação de serviço (DoS) e potencial execução remota de código.

Exploração

A exploração utiliza sequências específicas de frames HTTP/2 malformados para provocar falhas no gerenciamento interno de memória do Apache. O atacante envia múltiplas requisições manipuladas utilizando combinações específicas de HEADERS, RST_STREAM e streams simultâneos. A exploração pode resultar em:

- Queda de workers Apache
- Consumo excessivo de CPU e memória
- Interrupção de serviços web

- Instabilidade geral do servidor
- Possível execução remota de código em cenários específicos
- Impacto em aplicações hospedadas no mesmo ambiente

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Atualizar imediatamente para Apache HTTP Server 2.4.67
  - Desabilitar HTTP/2 temporariamente caso não seja essencial
  - Reiniciar serviços afetados após aplicação do patch
  - Monitorar instabilidade e falhas recorrentes
- **Recomendações para administradores de sistema:**
  - Revisar uso do módulo mod_http2
  - Implementar WAF com proteção contra abuso HTTP/2
  - Monitorar consumo de memória e workers Apache
  - Configurar rate limiting para conexões HTTP/2
  - Priorizar atualização de servidores expostos à internet
  - Implementar alta disponibilidade para minimizar impactos
- **Recomendações para administradores de sistema:**
  - Reportar indisponibilidade de aplicações web
  - Evitar reutilização de credenciais em sistemas afetados
  - Monitorar comportamento incomum em aplicações hospedadas

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://thehackernews.com/2026/05/critical-apache-http2-flaw-cve-2026.html.

2.5. Exposição de API Key Hardcoded no ClickUp expõe dados corporativos

Foi identificada uma API Key hardcoded em arquivos JavaScript públicos do ClickUp, acessíveis diretamente pelo navegador. Essa chave permitia comunicação com a API do Split.io sem autenticação adicional, expondo dados internos como e-mails corporativos e feature flags. O problema evidencia falhas no gerenciamento de segredos em aplicações SaaS.

Exploração

A exploração é simples e não exige acesso privilegiado. Um atacante pode:

- Inspecionar o código-fonte carregado no navegador
- Extrair a API Key exposta
- Realizar requisições diretas à API afetada
- Enumerar usuários, e-mails e configurações internas

Em cenários mais avançados, a vulnerabilidade SSRF associada poderia permitir:

- Acesso ao serviço de metadados cloud (ex: AWS)
- Coleta de credenciais temporárias
- Reconhecimento interno da infraestrutura
- Potencial movimentação lateral em ambientes cloud

Mitigação e Prevenção

- **Recomendações Imediatas:**
  - Revogar imediatamente a API Key exposta e rotacionar credenciais
  - Auditar acessos recentes à API para identificar possíveis abusos
  - Revisar integrações ativas que utilizam a chave comprometida
  - Aplicar correções no código para remover qualquer segredo exposto
- **Recomendações para Administradores de Sistema:**
  - Nunca armazenar secrets no frontend (JavaScript público)
  - Utilizar gerenciadores de segredos (ex: Vault, Secrets Manager)
  - Implementar backend intermediário para chamadas sensíveis à API
  - Aplicar princípio do menor privilégio em tokens e credenciais
  - Monitorar logs de API para detecção de uso anômalo
  - Bloquear acesso ao metadata service (169.254.169.254) quando não necessário
  - Implementar ferramentas de secret scanning no pipeline CI/CD
- **Recomendações para Usuários Finais:**
  - Ficar atento a e-mails suspeitos (possível uso em phishing direcionado)
  - Alterar senhas caso utilize integrações com a plataforma afetada
  - Habilitar MFA sempre que disponível
  - Reportar atividades incomuns ou acessos não reconhecidos

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/clickup-hardcoded-api-key-expose/.

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