Your IT Company

Principais Vulnerabilidades e Ameaças (Abril/25)

Sumário

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.

Vulnerabilidades e Ameaças descobertas

2.1. Vulnerabilidades em Active Directory e VPNs expostas

Pesquisadores de cibersegurança do grupo de inteligência de ameaças The DFIR Report descobriram um diretório aberto, acreditando estar associado a um afiliado do grupo de ransomware Fog. O servidor acessível publicamente revelou um arsenal sofisticado de ferramentas e scripts projetados para exploração de vulnerabilidades, roubo de credenciais e movimentação lateral, afetando diversos setores em diferentes regiões.

Exploração

O diretório analisado contém ferramentas especializadas para explorar vulnerabilidades do Active Directory (AD) e gain acesso inicial através de credenciais comprometidas da VPN SonicWall. Os scripts encontrados, como SonicWall Scanner, automatizam a autenticação em dispositivos VPN usando um arquivo estruturado com endereços IP, nomes de usuário, senhas e nomes de domínio. Após a conexão, as ferramentas permitem reconhecimento adicional da rede, facilitando a exploração de sistemas.

A presença de dados de vítimas no diretório, juntamente com evidências em sites de vazamento dedicados, destaca a seriedade da ameaça e o impacto em organizações vulneráveis.

Mitigação e Prevenção

Para se proteger contra essas ameaças, recomenda-se:

- **Atualização e Patch Management:** Implemente uma política rigorosa de gerenciamento de patches para corrigir vulnerabilidades conhecidas no Active Directory e VPNs utilizadas.
- **Reforço da Segurança de Endpoint:** Use soluções robustas de segurança de endpoint capazes de detectar e responder a atividades suspeitas.
- **Auditoria e Monitoramento:** Realize auditorias regulares de segurança e ative o monitoramento contínuo em busca de comportamento anômalo em redes e sistemas.
- **Educação de Funcionários:** Treine os colaboradores sobre segurança cibernética e reforço de senhas, para mitigar riscos associados ao roubo de credenciais.
- **Restrição de Acesso:** Limite os acessos a sistemas críticos e utilize autenticação multifator para proteger credenciais sensíveis.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://gbhackers.com/fog-ransomware-reveals-active-directory-exploitation/

Classificação: Público

2.2. Nova vulnerabilidade de DoS no Patch da Microsoft permite que usuários não administrativos bloqueiem atualizações de segurança

Recentemente, um patch de segurança da Microsoft, destinado a corrigir uma vulnerabilidade crítica de elevação de privilégios, introduziu acidentalmente uma nova falha significativa. Esta nova vulnerabilidade permite que usuários não administrativos bloqueiem permanentemente todas as atualizações de segurança do Windows, resultando em uma condição de negação de serviço (DoS).

Exploração

Em abril de 2025, a Microsoft lançou atualizações de segurança para corrigir a CVE-2025-21204, uma vulnerabilidade que permitia a um atacante autorizado escalar privilégios localmente, devido a um erro na resolução de links antes do acesso a arquivos. O patch implementado criou automaticamente uma pasta chamada "inetpub" em todos os sistemas Windows. No entanto, um pesquisador de segurança descobriu que este mesmo patch permite que usuários não administrativos, através da criação de um ponto de junção, bloqueiem o mecanismo de atualização do Windows, resultando em falhas nas instalações de atualizações de segurança.

Mitigação e Prevenção

- **Monitoramento de Ponto de Junção:** Administradores de sistema devem monitorar o drive do sistema (geralmente C:) em busca de pontos de junção incomuns que possam indicar tentativas de bloquear atualizações.
- **Bloqueio de Operações em Linha de Comando:** Restringir ou monitorar o acesso a operações na linha de comando pode dificultar a criação de junções por usuários não administrativos.
- **Educação do Usuário:** Treinamentos regulares sobre a importância de manter atualizações de segurança e o risco de exploração de vulnerabilidades devem ser realizados.
- **Revisão de Permissões:** Avaliar e, se possível, minimizar as permissões concedidas aos usuários padrão em ambientes críticos, para reduzir o risco de exploração.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/microsofts-symlink-patch-dos-vulnerability.

2.3. Campanha cibernética sofisticada alvo de servidores Microsoft-SQL vulneráveis

Uma nova campanha de ciberataques sofisticados está visando servidores Microsoft SQL (MS-SQL) mal gerenciados, com o objetivo de implantar ferramentas maliciosas como Ammyy Admin e malware PetitPotato. Essa ameaça ressalta a necessidade urgente de medidas de segurança robustas para proteger ambientes de banco de dados, que frequentemente são portas de entrada para dados organizacionais sensíveis.

Classificação: Público

Exploração

Os atacantes identificam e exploram servidores MS-SQL mal configurados ou desatualizados, utilizando credenciais fracas ou vulnerabilidades conhecidas para obter acesso não autorizado. Após a infiltração, eles executam comandos para coletar informações detalhadas do sistema, mapeando o ambiente para uma exploração adicional. Os atacantes então utilizam ferramentas como WGet para baixar e instalar payloads de malware, incluindo o Ammyy Admin e o PetitPotato, que permitem acesso remoto e escalonamento de privilégios. Esses métodos garantem que os invasores consigam manter uma presença nos sistemas comprometidos, facilitando movimentos laterais pela rede e aprofundando-se na infraestrutura crítica.

Mitigação e Prevenção

Para se defender contra esses ataques, especialistas em segurança recomendam:

- Realizar patches regulares nos servidores MS-SQL para corrigir vulnerabilidades conhecidas.
- Implementar mecanismos de autenticação fortes para limitar o acesso não autorizado.
- Desabilitar serviços desnecessários como o RDP quando não em uso.
- Monitorar a criação de contas suspeitas e a atividade da rede.
- Adotar uma postura de segurança em múltiplas camadas que combine proteção de endpoints, análise comportamental e monitoramento de rede, utilizando soluções de segurança como VMware Carbon Black Cloud.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://gbhackers.com/hackers-exploit-ms-sql-servers-to-deploy-ammyy-admin/

2.4 Nova ferramenta busca contornar autenticação em dois fatores do Microsoft Office 365

Pesquisadores de segurança descobriram uma nova e sofisticada ameaça para usuários do Microsoft Office 365: um kit de phishing como serviço chamado "SessionShark O365 2FA/MFA". Este toolkit é projetado para contornar as proteções de autenticação multifatorial (MFA), representando uma escalada alarmante na luta contínua entre defensores e atacantes cibernéticos.

Exploração

O SessionShark opera como uma plataforma de ataque "adversário no meio" (AiTM), direcionando-se para logins do Office 365. Sua principal função é a interceptação de cookies de sessão do usuário, que são os tokens que provam um login bem-sucedido via MFA. Ao roubar esses tokens, os atacantes podem sequestrar sessões autenticadas, tornando a MFA inútil mesmo que as credenciais originais e o código já tenham sido fornecidos pela vítima. A ferramenta apresenta técnicas de ocultação avançadas, garantindo que as páginas de phishing sejam vistas principalmente por usuários reais, diminuindo as chances de detecção.

Classificação: Público

Mitigação e Prevenção

- **Educação dos usuários**: Conscientize os membros da equipe sobre técnicas de phishing e como reconhecer tentativas de ataque.
- **Monitoramento de anomalias de sessão**: Esteja atento a comportamentos incomuns nas sessões de login dos usuários.
- **Defesas em camadas**: Considere implementar medidas adicionais de segurança além da MFA, como autenticação baseada em risco.
- **Utilização de sistemas de detecção**: Implementações de ferramentas de segurança devem ser atualizadas para identificar tentativas de fraude, como a utilização de CAPTCHAs em páginas de login.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://gbhackers.com/sessionshark-a-new-toolkit-bypasses-microsoft-office-365/

2.5 Vulnerabilidade crítica na Cisco pode levar a execução remota de código

A Cisco emitiu um aviso de alta severidade (cisco-sa-erlang-otp-ssh-xyZZy) sobre uma vulnerabilidade crítica de execução remota de código (RCE) em produtos que utilizam o servidor SSH do Erlang/OTP. Essa falha permite que atacantes não autenticados executem código arbitrário em dispositivos vulneráveis, tornando-se uma séria ameaça para redes empresariais e sistemas de telecomunicação.

Exploração

A vulnerabilidade, identificada como CVE-2025-32433, resulta de um tratamento inadequado das mensagens SSH durante a autenticação. Isso possibilita que os atacantes contornem as verificações de segurança e obtenham controle total sobre os sistemas afetados. Com uma pontuação CVSS de 10.0, a falha impacta produtos importantes da Cisco, como o Wide Area Application Services (WAAS) e o Network Services Orchestrator (NSO). Dispositivos não corrigidos podem ser alvos de ataques como ransomware, exfiltração de dados ou interrupções em operações críticas, representando riscos sistêmicos.

Mitigação e Prevenção

Para se proteger contra essa vulnerabilidade, a Cisco recomenda as seguintes ações:

- **Monitorar Atualizações:** Acompanhe os avisos para cronogramas de lançamento de patches.
- **Restringir Acesso SSH:** Limite a exposição bloqueando tráfegos SSH desnecessários.
- **Priorizar Patching:** Aplique correções imediatamente após sua disponibilidade.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://gbhackers.com/multiple-cisco-tools-at-risk/

Classificação: Público

2.6 Vulnerabilidade em plugin Category Posts Widget do WordPress pode permitir ataques XSS armazenados

O plugin Category Posts Widget do WordPress, em versões anteriores à 4.9.20, apresenta uma vulnerabilidade que não sanitiza e escapa alguns de seus settings. Isso pode permitir que usuários com privilégios elevados, como administradores, realizem ataques de Cross-Site Scripting (XSS) armazenados, mesmo quando a capacidade de HTML não filtrado está desativada, como em configurações de multisite.

Exploração

A vulnerabilidade ocorre devido à falha na sanitização dos dados inseridos nos settings do plugin. Usuários administradores podem injetar código malicioso que, quando armazenado, é executado em ambientes de fora, como em páginas acessadas por outros usuários. O impacto potencial inclui a possibilidade de execução de scripts maliciosos, comprometendo a segurança da aplicação e a privacidade dos usuários.

Mitigação e Prevenção:

- Atualize o plugin Category Posts Widget para a versão 4.9.20 ou superior para mitigar a vulnerabilidade.
- Realize auditorias de segurança regularmente em plugins e temas instalados, garantindo que todos estejam atualizados.
- Considere desabilitar o plugin se a atualização imediata não for uma opção.
- Para administradores de sistemas, implemente monitoramento de atividades suspeitas para detectar possíveis ataques XSS em tempo real.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://www.tenable.com/cve/CVE-2025-1453 e https://wpscan.com/vulnerability/6bf93a34-a19f-4266-a95d-033551db43e6/

2.7 Vulnerabilidade crítica no Google Chrome permite que atacantes escapem do sandbox

Uma vulnerabilidade crítica foi descoberta no Google Chrome, permitindo que atacantes quebrem o ambiente de proteção do sandbox do navegador. Essa falha, identificada como CVE-2025-2783, pode proporcionar acesso ao sistema operacional subjacente, colocando em risco a segurança de usuários em Windows, macOS e Linux.

Exploração

A vulnerabilidade se origina de um problema de corrupção de memória no mecanismo V8 do JavaScript do Chrome, permitindo a execução de código arbitrário dentro do ambiente sandbox. Os atacantes podem explorar essa fraqueza inicial e utilizar uma segunda falha na comunicação entre processos (IPC) para escalar privilégios e escapar do sandbox completamente.

Classificação: Público

Mitigação e Prevenção

Para mitigar esses riscos, as organizações devem:

- Atualizar o Google Chrome para a versão 134.0.6998.177 ou posterior.
- Verificar a versão do navegador acessando chrome://settings/help.
- Reiniciar o navegador após a atualização para garantir que o patch seja aplicado imediatamente.
- Implementar políticas de segurança adicionais que possam identificar e bloquear sites maliciosos.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/google-chrome-vulnerability-let-attackers-escape-payload-from-sandbox/

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 semanalmente.

Produzido por: Comitê Editorial de Segurança da Service Sec

Classificação: Público