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. Hackers Chineses Visam Sistemas Linux com Ferramentas Inovadoras

Um grupo de hackers vinculado à China, conhecido como UNC5174, lançou uma nova campanha utilizando uma variante do malware SNOWLIGHT e uma ferramenta open-source chamada VShell para infectar sistemas Linux. A relevância dessa ameaça está no uso crescente de ferramentas de código aberto, o que dificulta a atribuição de responsabilidade e torna as defesas mais complexas.

Exploração

O grupo UNC5174, anteriormente associado ao governo chinês, tem explorado falhas de segurança em softwares como Connectwise ScreenConnect e F5 BIG-IP. O malware SNOWLIGHT é um downloader que busca instalar um tunneler chamado GOHEAVY, enquanto a ferramenta VShell é um trojan de acesso remoto (RAT). A utilização de ferramentas de código aberto permite a esses atacantes operarem com um nível de sigilo e custo-efetividade, aumentando a complexidade da resposta de segurança.

Os ataques observados também envolveram o uso de um backdoor de shell reverso chamado GOREVERSE, bem como a exploração de falhas no Ivanti Cloud Service Appliance. Além disso, tanto o SNOWLIGHT quanto o VShell podem comprometer sistemas macOS, ampliando a gama de dispositivos-alvo.

Mitigação e Prevenção

Para se proteger contra esta nova ameaça, recomenda-se:

Administradores de Sistemas:

- Atualizar e aplicar patches de segurança relacionados ao Connectwise ScreenConnect, F5 BIG-IP e Ivanti Cloud Service Appliance.
- Monitorar e restringir o uso de ferramentas open-source em ambientes críticos, avaliando suas necessidades de segurança e compatibilidade.
- Implementar soluções de detecção de intrusões que possam identificar comportamentos suspeitos, como o uso de WebSockets para comunicação de comando e controle.

Usuários Finais:

- Evitar a instalação de aplicativos suspeitos, como ferramentas de autenticação que possam disfarçar malware.
- Manter sistemas operacionais e todos os softwares atualizados com as últimas correções de segurança.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://thehackernews.com/2025/04/chinese-hackers-target-linux-systems.html

2.2. Ameaças à Segurança: Explorações de 0-Day no Windows e Novas Táticas de Malware

Nesta semana, uma falha de 0-Day no Windows, CVE-2025-29824, foi explorada em ataques de ransomware, enquanto vulnerabilidades em softwares como ESET e Fortinet foram usadas para entregar malware e manter acesso a dispositivos. Essa situação enfatiza a necessidade de uma abordagem proativa em cibersegurança.

Exploração

A vulnerabilidade CVE-2025-29824, que afeta o Windows Common Log File System (CLFS), permite que atacantes obtenham privilégios de sistema. A exploração é feita através de um trojan chamado PipeMagic, utilizado para coleta de credenciais e entrega de cargas maliciosas, incluindo ransomwares, como o da família RansomEXX. Essa situação demonstra como o uso de ferramentas de segurança confiáveis pode ser comprometido e utilizado contra as próprias defesas.

Através de exploits em softwares de segurança como o ESET, os atacantes, identificados como parte do grupo ToddyCat, conseguiram executar cargas maliciosas em dispositivos infectados. Além disso, a Fortinet alertou sobre a manutenção do acesso a dispositivos FortiGate mesmo após a correção das vulnerabilidades, uma situação que ressalta a dificuldade de remediar brechas de segurança efetivamente.

Mitigação e Prevenção

- **Atualizações de Segurança**: Os usuários devem aplicar imediatamente as correções fornecidas pelas empresas de software, como a atualização do Patch Tuesday que tratou a CVE-2025-29824.
- **Monitoramento Proativo**: Implemente uma vigilância ativa para detectar atividades suspeitas, incluindo tentativas de uso de contas administrativas ou a ativação de contas que normalmente estão desativadas, como a conta de convidado do Windows.
- **Educação Continuada**: Treine as equipes sobre as novas táticas de ataques, incluindo phishing e exploração de vulnerabilidades em softwares de segurança.
- **Validação de Ferramentas de Segurança**: Avalie periodicamente a eficácia das ferramentas de segurança em uso para evitar que sejam exploradas por atacantes.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://thehackernews.com/2025/04/weekly-recap-windows-0-day-vpn-exploits.html

2.3. Campanha de Ataque Sofisticada Explora Mensagens do Microsoft Teams para Entregar Malware

Uma nova e sofisticada campanha de ataque está sendo perpetrada por cibercriminosos que exploram o Microsoft Teams para entregar malware e manter acesso persistente às redes corporativas. Os ataques representam uma evolução nas táticas de engenharia social e, em março de 2025, foram descobertos métodos de persistência previamente não vistos, como o "TypeLib hijacking", que representam uma ameaça significativa à segurança das empresas.

Exploração

Os atacantes se fazem passar por pessoal de suporte de TI, enviando mensagens de phishing aos funcionários pelo Teams, explorando o status de confiança da plataforma nas organizações. A técnica de "TypeLib hijacking" manipula o Registro do Windows para redirecionar objetos COM legítimos para scripts maliciosos hospedados em URLs externas, permitindo que os atacantes mantenham acesso persistente às máquinas alvo. Esta técnica foi observada em ataques reais e permite que a execução do código malicioso ocorra automaticamente após a reinicialização do sistema.

Mitigação e Prevenção

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

- Implementar controles rígidos sobre comunicações externas no Microsoft Teams.
- Habilitar autenticação multifatorial (MFA) para acessar contas e dados da empresa.
- Conduzir treinamentos regulares de conscientização para usuários sobre phishing e técnicas de engenharia social.
- Endurecer sistemas Windows para impedir a execução de código malicioso através da técnica de TypeLib hijacking.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/hackers-leveraging-teams-messages/

2.4 Nova vulnerabilidade crítica em plugin WordPress

Uma vulnerabilidade crítica no popular plugin WordPress SureTriggers foi explorada ativamente em apenas quatro horas após sua divulgação em 10 de abril de 2025. A falha de autenticação influencia todas as versões do plugin até a 1.0.78, permitindo que atacantes não autenticados criem contas de administrador em sites vulneráveis, potencialmente comprometendo todo o site.

Exploração

A vulnerabilidade se origina de uma falha crítica na forma como o SureTriggers lida com os endpoints da REST API. Especialistas em segurança identificaram que o plugin não valida corretamente cabeçalho HTTP ST-Authorization durante as requisições da API. Quando os atacantes enviam um cabeçalho inválido, o código do plugin retorna um valor nulo. Se o site não tiver configurado uma chave secreta interna (também nula por padrão), a verificação de autorização é inadvertidamente aprovada devido à comparação nula == nula, contornando completamente os protocolos de segurança.

Os ataques estão focalizados em dois endpoints específicos da API REST. A análise de segurança detectou várias tentativas de exploração originadas de múltiplos endereços IP, sendo eles: 2a01:e5c0:3167::2 (IPv6), 2602:ffc8:2:105:216:3cff:fe96:129f (IPv6), 89.169.15.201 (IPv4) e 107.173.63.224 (IPv4).

O principal objetivo dos atacantes parece ser estabelecer acesso persistente criando contas de administrador.

Mitigação e Prevenção

Os proprietários de sites que utilizam o plugin SureTriggers devem imediatamente atualizar para a versão mais recente. Aqueles que não puderem atualizar imediatamente devem desativar temporariamente o plugin até que uma atualização possa ser aplicada. Além disso, recomenda-se que os administradores façam o seguinte:

Auditem as contas de usuários para identificar quaisquer usuários de nível administrador suspeitos criados desde 10 de abril.

Verifiquem plugins, temas ou conteúdos recentemente instalados ou alterados.

Revisem os logs do servidor em busca de requisições nos endpoints vulneráveis.

Considerem implementar um firewall de aplicação web para proteção adicional.

Os clientes da Patchstack foram protegidos através do sistema de patch virtual da empresa, que bloqueou as tentativas de exploração antes que o patch oficial fosse lançado.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/wordpress-plugin-critical-vulnerability-exploited

2.5 Vulnerabilidade de Bypass de Anexos no Google Groups

Foi identificada uma vulnerabilidade significativa no Google Groups que permite que usuários contornem as restrições de anexos de arquivos ao enviar e-mails para endereços de grupos. Este problema de controle de acesso potencialmente afeta milhares de organizações que dependem do Google Groups para compartilhamento de informações controladas e colaboração.

Exploração

A vulnerabilidade observada por Ph.Hitachi explora uma desconexão entre duas funcionalidades do Google Groups: permissões para anexos e capacidades de postagem via e-mail. Mesmo quando os administradores do grupo restringem explicitamente as permissões de upload de arquivos para "apenas proprietários", membros regulares conseguem contornar essa restrição enviando um e-mail com anexos para o endereço do grupo. A configuração "Permitir Postagens por E-mail" possibilita que membros contribuam para discussões, mas falha em aplicar as restrições de anexos configuradas nas definições do grupo. Esse tipo de falha representa um grave problema de controle de acesso, onde as verificações de permissão não são aplicadas de forma consistente entre os diferentes métodos de acesso ao mesmo recurso.

Mitigação e Prevenção

Para mitigar essa vulnerabilidade, recomenda-se que os administradores do Google Workspace:

Implementem controles de acesso abrangentes e pratiquem a categorização adequada dos dados para limitar a exposição de informações confidenciais.

Revisem regularmente as configurações dos grupos para entender as implicações de segurança de funcionalidades como a postagem por e-mail.

Considerem desabilitar a configuração "Permitir Postagens por E-mail" se não for essencial, especialmente em grupos que lidam com informações sensíveis.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/google-groups-attachment-bypass-vulnerability/

2.6 Campanha Cibercriminosa Explora Vulnerabilidade de Metadados do EC2 da AWS

Uma campanha sofisticada de cibercriminosos tem como alvo sites hospedados em instâncias EC2 da Amazon Web Services (AWS), explorando uma vulnerabilidade nos Metadados do EC2 por meio de Server-Side Request Forgery (SSRF). Esta ameaça, observada em março de 2025, permite que atacantes acessem informações sensíveis, incluindo credenciais de papéis IAM, e potencialmente escalem seus ataques.

Exploração

Os atacantes estão utilizando duas vulnerabilidades comuns: CWE-200, que se refere à exposição de informações sensíveis para atores não autorizados, e CWE-918, que diz respeito ao SSRF. Eles enviam requisições GET para sites hospedados em instâncias EC2 e tentam recuperar metadados a partir do endereço IP interno (169.254.169.254). Os metadados contêm informações críticas, como credenciais de papéis IAM, que podem ser usadas para acessar recursos da AWS de forma não autorizada. A exploração desta vulnerabilidade, especialmente através do IMDSv1, coloca em risco a segurança dos ambientes AWS, uma vez que os dados do IMDSv1 não são protegidos por métodos de autenticação ou criptografia.

Para mitigar essa ameaça, os usuários da AWS devem:

- Transitionar de IMDSv1 para IMDSv2: O IMDSv2 requer que os atacantes forneçam um token secreto, reduzindo significativamente o risco de ataques baseados em SSRF;
- Implementar regras de Firewall de Aplicação Web (WAF): Essas regras devem bloquear solicitações ao IP do serviço de metadados para prevenir acessos não autorizados;
- Manter as configurações de nuvem seguras e atualizadas: As organizações precisam ser diligentes em garantir que suas configurações de nuvem estejam protegidas contra vulnerabilidades conhecidas.

IOCs:

Endereço IP: Diversos IPs associados ao Autonomous System Number (ASN) da FBW NETWORKS SAS.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://gbhackers.com/cybercriminals-exploit-ec2-instance-metadata-vulnerability/

2.7 Vulnerabilidades Críticas no Windows Task Scheduler Permitindo Bypass de UAC e Evasão de Detecção

Recentemente, novas vulnerabilidades foram descobertas no Windows Task Scheduler, especificamente no utilitário schtasks.exe, que permitem a atacantes contornar a UAC (User Account Control), alterar metadados, modificar logs de eventos e evadir detecções. Esse conjunto de vulnerabilidades pode ser explorado para manter acesso não autorizado e evitar registros de atividades maliciosas.

Exploração

As principais vulnerabilidades incluem um bypass de UAC que permite que atacantes com credenciais de administrador local executem comandos com privilégios de SYSTEM sem gerar um aviso de UAC, mesmo em configurações mais rigorosas. Ao criar uma tarefa agendada utilizando a autenticação de Batch Logon, os atacantes podem explorar mecanismos de impersonação do serviço Task Scheduler, que opera como SYSTEM, concedendo privilégios máximos ao sistema. Além disso, técnicas de evasão de detecção, como a manipulação de metadados de tarefas e contaminação de logs de eventos, permitem que os atacantes ocultem suas atividades e apaguem evidências de ações maliciosas.

Mitigação e Prevenção

Para mitigar esses riscos, as organizações devem:

- Aplicar controles de acesso rigorosos às tarefas agendadas.
- Desabilitar NTLM onde for possível, preferindo o uso de autenticação Kerberos.
- Monitorar ativamente a atividade do Task Scheduler em busca de anomalias.
- Implementar princípios de menor privilégio para limitar o acesso de contas de usuários.
- Realizar uma gestão de patches regular para manter o software atualizado e corrigido contra vulnerabilidades.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://gbhackers.com/windows-task-scheduler-vulnerabilities/

2.8 Cuidado com Conversores de PDF Online Falsos que Enganam Usuários

Uma nova campanha de malware oriunda de sites fraudulentos que prometem converter PDFs para DOCX está enganando usuários desavisados. Esses sites imitam serviços legítimos, como o PDFCandy, e utilizam táticas de engenharia social para roubar informações sensíveis, como credenciais de browsers e detalhes de carteiras de criptomoedas.

Exploração

Os cibercriminosos têm aproveitado o aumento da demanda por ferramentas de conversão de documentos, criando sites enganosos como candyxpdf[.]com e candyconverterpdf[.]com. Após o upload de um arquivo, o usuário é induzido a executar um comando PowerShell disfarçado através de uma CAPTCHA falsa. Esse comando inicia uma cadeia de infecção, resultando na instalação do malware ArechClient2, uma variante da famigerada família SectopRAT. Este malware é projetado para roubar informações sensíveis e liberdade do sistema, utilizando técnicas de evasão avançadas para contornar controles de segurança.

Mitigação e Prevenção

Para se proteger contra essa ameaça, recomenda-se:

- Utilizar somente ferramentas de conversão de arquivos confiáveis: Acesse páginas oficiais de serviços conhecidos e evite sites desconhecidos.

- Cuidado com comandos executados: Nunca execute comandos de um site que pareça suspeito, mesmo que a interface pareça legítima.
- Manter software de segurança atualizado: Utilize um bom antivírus e ferramentas de detecção de malware.
- Conscientização do usuário: Educar usuários sobre os riscos de engenharia social e como reconhecer sinais de fraudes online.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/beware-of-online-pdf-converters-that-tricks-users/

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: Comitê Editorial de Segurança da Service Sec