Your IT Company

Principais Vulnerabilidades e Ameaças (Fevereiro/25)

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. Malware furtivo em sites WordPress permite a execução remota de código por hackers

Pesquisadores de segurança identificaram uma nova variante de malware altamente sofisticado, projetado especificamente para comprometer sites WordPress por meio de backdoors ocultos, viabilizando a execução remota de código (RCE).

Os ataques exploram vulnerabilidades críticas em componentes essenciais do ecossistema WordPress, incluindo plug-ins, temas e permissões inadequadamente configuradas. Uma vez exploradas, essas falhas permitem que invasores obtenham acesso persistente, executem código arbitrário e escalem privilégios para manter controle total do ambiente comprometido. Além disso, o malware emprega técnicas avançadas de ofuscação e anti-análise para evadir mecanismos de detecção e remoção.

Essas descobertas ressaltam a urgência de estratégias defensivas robustas, incluindo a aplicação rigorosa de patches, endurecimento da superfície de ataque, monitoramento contínuo de atividades suspeitas e adoção de práticas como a implementação de políticas de segurança Zero Trust para mitigar riscos em infraestruturas WordPress.

Exploração

Os Pesquisadores identificaram uma campanha sofisticada na qual atacantes exploram o diretório Must-Use Plugins (mu-plugins) do WordPress para garantir persistência furtiva e execução remota de código. Esse diretório, projetado para carregar automaticamente qualquer script PHP presente nele sem necessidade de ativação manual, foi utilizado de forma estratégica para comprometer sistemas sem levantar suspeitas.

Os invasores implantaram scripts PHP altamente ofuscados, empregando múltiplas camadas de codificação base64, compressão Gzip e criptografia AES, tornando a análise e detecção significativamente mais complexa. Além disso, o código malicioso possuía mecanismos de mutação, alterando sua estrutura a cada execução para evitar detecções baseadas em assinaturas.

Uma vez inserido no diretório mu-plugins, o malware estabelecia um canal seguro de comunicação com servidores de comando e controle (C2). Esse canal permitia a execução remota de comandos arbitrários, o download dinâmico de payloads adicionais e a exfiltração de dados sensíveis, expandindo o comprometimento do ambiente.

Os atacantes também empregaram técnicas avançadas para dificultar sua remoção e análise, incluindo:

- Abuso de funções PHP dinâmicas (eval(), assert(), create_function(), preg_replace('/.*/e')) para executar código arbitrário em tempo de execução.
- Deserialização insegura, permitindo a reconstrução de objetos maliciosos a partir de entradas aparentemente inofensivas.

Classificação: Público

- Execução modular, na qual o malware recuperava cargas adicionais apenas quando necessário, reduzindo sua pegada e evitando análises estáticas.
- Evasão de logs e ocultação de tráfego, utilizando técnicas como encapsulamento de comunicações em requisições HTTP legítimas.

Em um dos incidentes analisados, o malware explorou o diretório /wp-content/uploads/ para armazenar cargas úteis altamente ofuscadas, aproveitando a permissividade desse local, frequentemente configurado com permissões de escrita liberadas.

Essas cargas foram posteriormente decodificadas e executadas diretamente no servidor, permitindo que os invasores estabelecessem persistência, executassem código arbitrário e obtivessem controle total sobre o ambiente comprometido. A técnica possibilitou a execução remota sem levantar suspeitas, uma vez que os arquivos armazenados no diretório de uploads geralmente não são monitorados por mecanismos de segurança tradicionais.

Além disso, variantes mais sofisticadas do malware manipularam arquivos críticos para diferentes finalidades maliciosas, incluindo:

- Redirecionamento de tráfego, modificando arquivos como .htaccess e injectando regras de reescrita para direcionar visitantes para páginas controladas pelos atacantes.
- SEO Black Hat, alterando o robots.txt para indexar páginas fraudulentas, favorecendo campanhas de manipulação de motores de busca. Essa técnica permitiu que os atacantes aumentassem a visibilidade de sites maliciosos, prejudicando a reputação e o ranqueamento do site comprometido.

Esse ataque demonstra como invasores exploram diretórios com permissões mal configuradas para ocultar cargas maliciosas e comprometer sites WordPress de maneira furtiva. Para mitigar esse tipo de ameaça, é essencial restringir permissões de escrita, monitorar atividades suspeitas no diretório de uploads e implementar verificações de integridade para detectar modificações não autorizadas em arquivos críticos.

As consequências potenciais dos ataques são graves, o atacante poderá ter a aquisição completa do site, roubar os dados, distribuir malwares e consequentemente causar danos a reputação, prejudicando principalmente sites que possuem classificação de SEO.

Mitigação e prevenção

Diante da sofisticação dessa ameaça, abordagens tradicionais de segurança se mostram insuficientes. Medidas avançadas para mitigar ataques dessa natureza incluem:

Atualize regularmente o núcleo, os plug-ins e os temas do WordPress.

Implemente firewalls para bloquear o tráfego malicioso.

Desative a execução do PHP em diretórios como ./uploads/

Use ferramentas de segurança como Sucuri ou MalCare para verificação e monitoramento de malware.

Realize auditorias periódicas de plug-ins instalados e remova os não utilizados ou desatualizados.

Essas medidas são essenciais para reduzir a superfície de ataque e proteger contra ameaças cibernéticas em evolução direcionadas aos ecossistemas WordPress.

Classificação: Público

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://gbhackers.com/stealthy-malware-in-wordpress-sites-enables/ e https://blog.sucuri.net/2025/02/hidden-backdoors-uncovered-in-wordpress-malware-investigation.html

2.2. Alerta de Segurança: CISA emite alerta sobre vulnerabilidade crítica no Palo Alto Firewall CVE-2025-0108

A Agência de Segurança Cibernética e Infraestrutura (CISA) emitiu um alerta urgente sobre a exploração ativa da vulnerabilidade CVE-2025-0108, uma falha de desvio de autenticação de alta gravidade no Palo Alto.

Networks PAN-OS, sistema operacional dos dispositivos de firewall da empresa.

Exploração

Desde 13 de fevereiro, pesquisadores de inteligência de ameaças, registrou um aumento nas tentativas de exploração da falha, saltando de 2 para 25 IPs maliciosos em apenas cinco dias. O tráfego de ataque tem origem predominante nos Estados Unidos, Alemanha e Holanda.

Autoridades federais alertam que invasores podem encadear essa falha com outras vulnerabilidades para comprometer infraestruturas críticas de rede. Segundo a Palo Alto Networks, a vulnerabilidade pode ser combinada com a falha CVE-2024-9474 para um comprometimento total do dispositivo.

Detalhes da Vulnerabilidade

O CVE-2025-0108, com pontuação CVSSv3.1 de 7.8, permite que invasores não autenticados com acesso à interface da Web de gerenciamento do PAN-OS ignorem os controles de autenticação e executem scripts PHP específicos. Embora não possibilite diretamente a execução remota de código, a falha compromete a integridade e confidencialidade do sistema.

As versões afetadas incluem:

- PAN-OS 10.1 (antes de 10.1.14-h9)
- PAN-OS 10.2 (antes de 10.2.13-h3)
- PAN-OS 11.1 (antes de 11.1.6-h1)
- PAN-OS 11.2 (antes de 11.2.4-h4)
- As implementações Cloud NGFW e Prisma Access não são impactadas.

Mitigação e prevenção

A CISA e a Palo Alto Networks recomendam que todas as organizações tomem as seguintes ações imediatas:

Aplique os patches disponíveis: Atualize para as versões 10.1.14-h9, 10.2.13-h3, 11.1.6-h1 ou 11.2.4-h4.

Restrinja o acesso à interface de gerenciamento: Limite a conectividade a endereços IP internos confiáveis, evitando exposição à Internet.

Desative serviços não utilizados: O plug-in OpenConfig deve ser desativado se não for essencial.

Monitore tentativas de exploração: Utilize plataformas de inteligência de ameaças, como o GreyNoise, para rastrear atividades maliciosas.

Classificação: Público

O pesquisador, destacou que a maior ameaça do CVE-2025-0108 é seu uso como vetor de acesso inicial, permitindo que invasores executem ataques secundários para comprometer os dispositivos.

Diante da escalada da exploração ativa, organizações e agências federais devem priorizar a aplicação dos patches. A CISA reforça sua iniciativa "Secure by Design", incentivando fornecedores e clientes a eliminarem vulnerabilidades na infraestrutura crítica.

O porta-voz da Palo Alto Networks, Steven Thai, reforçou o apelo: "Pedimos a todos os clientes que apliquem imediatamente as atualizações e restrinjam o acesso à interface de gerenciamento".

Com ataques em crescimento, especialistas alertam que firewalls não corrigidos estão sob risco iminente de comprometimento. Administradores de sistemas devem agir rapidamente para mitigar a ameaça e reforçar seus controles de segurança.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://cybersecuritynews.com/pan-os-vulnerability-actively-exploited

2.3. Novas falhas do OpenSSH permitem ataques Man-in-the-Middle e DoS — Patch Now.

Duas vulnerabilidades de segurança foram descobertas no pacote de utilitários de rede segura OpenSSH que, se exploradas com sucesso, podem resultar em um ataque ativo de máquina no meio (MitM) e um ataque de negação de serviço (DoS), respectivamente, sob certas condições.

As vulnerabilidades, detalhadas pela Qualys Threat Research Unit (TRU), estão listadas abaixo:

- CVE-2025-26465 (pontuação CVSS: 6,8) - O cliente OpenSSH contém um erro lógico entre as versões 6.8p1 a 9.9p1 (inclusive) que o torna vulnerável a um ataque MitM ativo se a opção VerifyHostKeyDNS estiver habilitada, permitindo que um intruso mal-intencionado se passe por um servidor legítimo quando um cliente tenta se conectar a ele (introduzido em dezembro de 2014).
- CVE-2025-26466 (pontuação CVSS: 5,9) - O cliente e o servidor OpenSSH são vulneráveis a um ataque DoS de pré-autenticação entre as versões 9.5p1 a 9.9p1 (inclusive) que causa consumo de memória e CPU (introduzido em agosto de 2023).

"Se um invasor puder realizar um ataque man-in-the-middle via CVE-2025-26465, o cliente poderá aceitar a chave do invasor em vez da chave do servidor legítimo", disse Saeed Abbasi, gerente de produto da Qualys TRU.

"Isso quebraria a integridade da conexão SSH, permitindo uma possível interceptação ou adulteração da sessão antes mesmo que o usuário perceba."

Exploração

A falha CVE-2025-26465 permite ataques man-in-the-middle (MitM), nos quais um atacante pode redirecionar a conexão SSH de um utilizador para um servidor controlado, em vez do destino legítimo, o que pode resultar no roubo de credenciais ou de outras informações confidenciais.

Classificação: Público

O sucesso do ataque depende da configuração da opção VerifyHostKeyDNS no cliente OpenSSH, que deve estar definida como “sim” ou “perguntar”. Embora, por predefinição, esta opção esteja desativada, sistemas como o FreeBSD mantiveram-na ativa por padrão entre 2013 e 2023, aumentando a exposição ao risco.

Já a vulnerabilidade CVE-2025-26466, presente desde 2023, pode ser explorada para desencadear ataques de negação de serviço (DoS) contra clientes e servidores OpenSSH. Um atacante pode esgotar os recursos de memória enviando um elevado número de pings e chaves de host de servidor com extensões de certificado adicionais, levando a uma falha na troca de chaves e permitindo a ligação a servidores não verificados.

Uma exploração bem-sucedida pode permitir que agentes mal-intencionados comprometam e sequestrem sessões SSH e obtenham acesso não autorizado a dados confidenciais. Vale a pena notar que a opção VerifyHostKeyDNS está desabilitada por padrão.

Dito isso, a opção foi habilitada por padrão no FreeBSD de setembro de 2013 a março de 2023, expondo potencialmente as máquinas que executam o sistema operacional semelhante ao Unix a riscos potenciais.

A exploração repetida do CVE-2025-26466, por outro lado, pode resultar em problemas de disponibilidade, impedindo que os administradores gerenciem servidores e bloqueiem usuários legítimos, prejudicando efetivamente as operações de rotina.

Mitigação e prevenção

Dado o impacto potencial destas falhas, a Qualys recomenda a atualização imediata para o OpenSSH 9.9p2. Além disso, a mitigação pode ser feita desativando o VerifyHostKeyDNS para reduzir o risco associado ao CVE-2025-26465 e ajustando parâmetros como LoginGraceTime, MaxStartups e PerSourcePenalties para dificultar a exploração do CVE-2025-26466 em servidores OpenSSH.

A presença do OpenSSH em múltiplos sistemas Unix-like, incluindo Linux e macOS, torna estas falhas particularmente preocupantes. A Qualys já havia identificado, em julho de 2024, uma vulnerabilidade de execução remota de código (RCE) no OpenSSH, designada regreSSHion, que expôs milhões de servidores na Internet.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://thehackernews.com/2025/02/new-openssh-flaws-enable-man-in-middle.html e https://www.itsecurity.pt/news/threats/vulnerablidades-no-openssh-expoem-utilizadores-a-ataques-mitm-e-dos

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

Classificação: Público