Your IT Company

Principais Vulnerabilidades e Ameaças (Dezembro/24)

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. Falhas no plugin Anti-Spam da CleanTalk expõe sites WordPress para ataques remotos

Anti-Spam da CleanTalk é um plugin baseado em nuvem projetado para proteger sites contra spam em formulários, comentários e registros de usuários. Ele utiliza algoritmos avançados para analisar o comportamento e os dados enviados por visitantes, bloqueando automaticamente ações suspeitas, como mensagens de spam e bots automatizados.

A ferramenta não usa CAPTCHA, o que melhora a experiência do usuário legítimo. É compatível com diversas plataformas de sites, como WordPress, oferecendo relatórios detalhados de spam bloqueado e integração fácil.

Recentemente duas vulnerabilidades críticas foram descobertas no plugin afetando versões até 6.44 e expondo mais de 200.000 sites a ataques.

A primeira recebeu a identificação CVE-2024-10542 sendo classificada com severidade crítica, e pontuação 9.8 na métrica de classificação CVSS v3.1 pela Wordfence, tendo a seguinte descrição: “O plugin Spam protection, Anti-Spam, FireWall by CleanTalk para WordPress é vulnerável à instalação arbitrária de plugins não autorizada devido a um bypass de autorização por meio de spoofing de DNS reverso na função checkWithoutToken em todas as versões até a 6.43.2. Essa vulnerabilidade permite que atacantes não autenticados instalem e ativem plugins arbitrários, o que pode ser explorado para alcançar execução remota de código (RCE) caso outro plugin vulnerável seja instalado e ativado.”

Permitindo que invasores não autenticados instalem e ativem plugins arbitrários. A exploração ocorre devido a verificações inadequadas no método checkWithoutToken(), que aceita IPs forjados para simular origens confiáveis, como subdomínios falsos de cleantalk.org. Essa falha pode ser usada para alcançar execução remota de código caso outros plugins vulneráveis estejam presentes.

A segunda recebeu a identificação CVE-2024-10781 sendo classificada também com severidade crítica, e pontuação 9.8 na métrica de classificação CVSS v3.1 pela Wordfence, tendo a seguinte descrição: “O plugin Spam protection, Anti-Spam, FireWall by CleanTalk para WordPress é vulnerável à instalação arbitrária de plugins não autorizada devido à ausência de uma verificação de valor vazio no parâmetro api_key na função perform em todas as versões até a 6.44. Essa vulnerabilidade permite que atacantes não autenticados instalem e ativem plugins arbitrários, o que pode ser explorado para alcançar execução remota de código (RCE) caso outro plugin vulnerável seja instalado e ativado.”

Assim permitindo a exploração da ausência de validação quando a chave de API que está ausente, permitindo que invasores realizem ações críticas sem autenticação, como instalação de plugins maliciosos.

Exploração e Proof-of-Concept (PoC)

- Spoofing de DNS Reverso: O atacante manipula cabeçalhos HTTP como X-Forwarded-By e X-Client-IP para forjar um domínio subjacente, que inclui a string cleantalk.org. O método gethostbyaddr() aceita o domínio falso, passando pela verificação de autorização.
- Execução de Comandos Maliciosos: O atacante explora o endpoint perform() para realizar ações administrativas, como ativar plugins maliciosos.

```
POST /wp-admin/admin-ajax.php?action=perform&plugin_name=malicious-plugin HTTP/1.1
Host: vulnerable-site.com
X-Forwarded-By: attacker.evil-cleantalk.org
```

Esse comando instala e ativa um plugin malicioso que pode incluir backdoors ou ferramentas para controle remoto.

Mitigação e Prevenção

É extremamente recomendado atualizar para a versão 6.45 ou mais recente, que já contém correções para ambas as vulnerabilidades além de se certificar que a chave de API do CleanTalk esteja configurada corretamente para evitar ataques baseados em valores nulos.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://www.wordfence.com/blog/2024/11/200000-wordpress-sites-affected-by-unauthenticated-critical-vulnerabilities-in-anti-spam-by-cleantalk-wordpress-plugin/ , https://nvd.nist.gov/vuln/detail/CVE-2024-10781 e https://nvd.nist.gov/vuln/detail/CVE-2024-10542

2.2. Vulnerabilidade crítica na validação de certificados no app GlobalProtect da Palo Alto permite ataques de escalação de privilégios

Foi identificada uma vulnerabilidade crítica no aplicativo GlobalProtect da Palo Alto Networks, que pode permitir a elevação de privilégios por atacantes em sistemas afetados. Essa falha representa um risco significativo à segurança, podendo ser explorada para comprometer a integridade e o controle dos ambientes vulneráveis.

A vulnerabilidade foi identificada como CVE-2024-5921 e está classificada pela Palo Alto com uma pontuação de nível médio CVSS 5.6 e que possui a seguinte descrição, “Um problema de validação de certificação insuficiente no aplicativo Palo Alto Networks GlobalProtect permite que os invasores conectem o aplicativo GlobalProtect a servidores arbitrários. Isso pode permitir que um usuário do sistema operacional local não administrativo ou um invasor na mesma sub-rede instale certificados raiz mal-intencionados no ponto de extremidade e, posteriormente, instale software mal-intencionado assinado pelos certificados raiz mal-intencionados nesse ponto de extremidade”. Esta CVE ainda não foi classificada pelo NIST.

A vulnerabilidade afeta várias versões do aplicativo GlobalProtect, incluindo:

- Todas as versões do GlobalProtect App 6.3, 6.1, 6.0 e 5.1
- GlobalProtect App 6.2 versões anteriores a 6.2.6 no Windows
- Todas as versões do GlobalProtect App 6.2 no macOS e Linux
- Todas as versões do aplicativo GlobalProtect UWP no Windows

Exploração

A Palo Alto Networks não tem conhecimento de nenhuma exploração maliciosa desse problema, entretanto, o impacto potencial segue significativo.

Mitigação e Prevenção:

A mitigação desse problema pode ser implementada em todas as plataformas compatíveis (Windows, macOS, Linux, iOS e Android) configurando o aplicativo GlobalProtect 6.0 no modo FIPS-CC ou utilizando o GlobalProtect 5.1 também no modo FIPS-CC. Para detalhes técnicos, consulte a tabela "Validação da Certificação FIPS-CC" disponível em nossa documentação oficial.

Observação técnica: Essa solução alternativa é específica para a configuração do modo FIPS-CC no aplicativo GlobalProtect. Não há relação com configurações FIPS-CC aplicadas em portais ou gateways do GlobalProtect. Portanto, não é necessário que os portais ou gateways estejam configurados no modo FIPS-CC para que essa mitigação seja aplicada com eficácia.

A vulnerabilidade foi corrigida na versão 6.2.6 do aplicativo GlobalProtect para Windows e em todas as versões subsequentes da série 6.2. Correções adicionais estão em desenvolvimento e serão lançadas para as demais plataformas compatíveis, incluindo macOS, Linux, iOS e Android.

A implementação da correção para essa vulnerabilidade requer as seguintes etapas:

- Verifique se todos os portais do GlobalProtect utilizam cadeias de certificados TLS compostas exclusivamente por certificados X.509v3 válidos, de acordo com os padrões de conformidade estabelecidos.
- Certifique-se de que as cadeias de certificados TLS usadas pelos portais do GlobalProtect estejam configuradas no repositório de certificados raiz do sistema operacional utilizado nos dispositivos cliente.
- Instale uma versão corrigida do aplicativo GlobalProtect seguindo as opções de implantação fornecidas. Essa versão reforça verificações estritas de conformidade X.509v3 nos certificados fornecidos pelos portais GlobalProtect, mitigando a exploração da vulnerabilidade.

Os administradores podem utilizar ferramentas de gerenciamento de dispositivos móveis (MDM) ou de endpoints para aplicar as configurações necessárias.

Siga os passos abaixo para garantir a instalação e configuração correta do GlobalProtect

- Baixe e instale a versão mais recente e corrigida do aplicativo GlobalProtect, garantindo compatibilidade e mitigação de possíveis vulnerabilidades.

- Altere as configurações no Registro conforme os parâmetros recomendados abaixo:

Caminho: HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings
Valores:
cert-store: machine
cert-location: ROOT
full-chain-cert-verify: yes

Após aplicar as alterações no Registro, é obrigatório reiniciar o sistema operacional para que as novas configurações sejam efetivamente aplicadas.

Adotar essas medidas preventivas não apenas mitiga a vulnerabilidade atual, mas também fortalece a segurança geral do ambiente.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://cybersecuritynews.com/palo-alto-certificate-validation-flaw/ e https://security.paloaltonetworks.com/CVE-2024-5921

2.3. Falha em componente da Red Hat OpenStack Platform permite ataques man-in-the-middle.

O Red Hat OpenStack Platform (RHOSP) é uma plataforma de infraestrutura como serviço (IaaS) baseada no OpenStack, desenvolvida pela Red Hat, que oferece uma solução escalável, altamente disponível e pronta para produção para implantar e gerenciar nuvens privadas e públicas. Inclui integração com tecnologias da Red Hat, como o Red Hat Enterprise Linux (RHEL), para garantir segurança e estabilidade.

O componente openstack-tripleo-common do RHOSP Director é uma ferramenta usada para implantar, gerenciar e escalar o OpenStack. O tripleo-common fornece bibliotecas e scripts comuns que suportam operações de automação, personalização e atualização no processo de gerenciamento do OpenStack Director. Ele centraliza funções reutilizáveis para facilitar a implantação e manutenção.

Uma falha foi encontrada no componente openstack-tripleo-common do diretor Red Hat OpenStack Platform (RHOSP). Essa vulnerabilidade permite que um invasor implante imagens de contêiner potencialmente comprometidas por meio da desativação da verificação de certificado TLS para espelhos de registro, o que pode permitir um ataque man-in-the-middle (MITM) afetando as versões do Red Hat OpenStack Platform (RHOSP) 16.1 e 16.2.

Esta falha recebeu a identificação CVE-2024-8007 sendo classificada com severidade alta, e pontuação 8.1 na métrica de classificação CVSS v3.1 pela Red Hat, tendo a seguinte descrição: “Foi identificada uma falha no componente openstack-tripleo-common da Red Hat OpenStack Platform (RHOSP) director. Essa vulnerabilidade permite que um atacante implante imagens de contêiner potencialmente comprometidas ao desativar a verificação do certificado TLS para espelhos de registro, o que pode possibilitar um ataque de man-in-the-middle (MITM).”

O Diretor do RHOSP possui uma etapa "container image prepare" que gera um arquivo de configuração de implantação contendo a lista de imagens de contêiner a serem implantadas nos nós do OSP com base na configuração fornecida pelo usuário. Ele pode, opcionalmente, preencher um registro local e atualizar o arquivo de configuração para referenciar as imagens espelhadas localmente.

Exploração

- Desativação da verificação TLS:

Se a verificação TLS dessa conexão falhar, o registro é automaticamente adicionado ao parâmetro DockerInsecureRegistries no arquivo de configuração gerado."

Isso implica que, quando ocorre uma falha na verificação TLS, a plataforma desativa a verificação de segurança para o registro, tornando a comunicação com o registro insegura.

- Ajuste de configuração insegura:

Esse parâmetro definirá, em última instância, insecure=true para o registro referenciado em /etc/containers/registry.conf em todos os hosts durante a implantação/atualização do RHOSP, e as imagens serão baixadas do registro de forma insegura."

A falha na verificação TLS adiciona o registro à lista de registros inseguros, o que permite que imagens sejam baixadas sem a devida validação de segurança. Esse processo pode ser explorado para que imagens comprometidas sejam entregues sem detecção.

- Espelhamento de imagens:

"Se a verificação TLS dessa conexão falhar, a verificação TLS será desativada para a tarefa de espelhamento da imagem."

Quando a TLS falha no espelhamento de imagens, a verificação TLS é desativada, permitindo que o espelhamento seja feito sem qualquer segurança, o que pode ser explorado por um atacante para inserir imagens corrompidas.

A exploração ocorre quando a verificação TLS falha, o que leva à desativação da segurança nas conexões com os registros de contêiner. Como resultado, os registros são considerados inseguros, e o parâmetro DockerInsecureRegistries é ativado, permitindo que imagens sejam baixadas sem qualquer verificação de autenticidade. No processo de espelhamento de imagens, essa falha na verificação TLS também desativa a segurança, possibilitando que um invasor entregue imagens de contêiner corrompidas ou comprometidas sem que o sistema detecte a manipulação. Isso configura uma vulnerabilidade crítica, pois um ataque Man-in-the-Middle (MITM) poderia ser realizado, e o conteúdo comprometido seria implantado nos nós do OpenStack sem qualquer sinal de alerta.

Esse aumento de explicação detalha melhor como o processo de falha na verificação TLS é aproveitado por um atacante para introduzir riscos de segurança.

Mitigação/Prevenção

A Red Hat já lançou uma versão corrigida do RHOSP, disponível em versões 17.1 e superiores. Certifique-se de aplicar essas atualizações para corrigir a falha de verificação TLS.

Reforce a validação de TLS e utilize registros de imagens de contêiner confiáveis e com autenticação adequada.

Implemente ferramentas de monitoramento de rede para detectar tráfego suspeito e comunicações com espelhos de registro não seguros.

Revise e audite as configurações do RHOSP para garantir que apenas registros de contêiner seguros estejam sendo utilizados, e que qualquer falha de TLS seja devidamente tratada e não permita a injeção de imagens comprometidas.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir:
https://nvd.nist.gov/vuln/detail/cve-2024-8007 ,
https://bugzilla.redhat.com/show_bug.cgi?id=2305975 e
https://access.redhat.com/security/cve/CVE-2024-8007

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