

Consultoria de segurança do Catalyst SD-WAN de correção - setembro de 2026

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Visão Geral do Fluxo de Trabalho de Correção](#)

[Passo 1: Coletar arquivos de administração técnica de todos os gerentes](#)

[Alternativa: Verificação manual \(somente se não for possível coletar Admin-Tech\)](#)

[Passo 2: Atualizar para uma versão de software fixo](#)

[Passo 3: Abra um caso no TAC e carregue os arquivos do Admin-Tech para verificação](#)

[Passo 4: Se o comprometimento for identificado — Diretrizes do TAC](#)

[Versões de software fixo](#)

[Anexo: Etapas de verificação manual \(somente se a coleta de Admin-Tech não for possível\)](#)

[Como identificar os indicadores de comprometimento](#)

[Verificação 1: Auditoria do Log de Acesso ao Proxy de Serviço](#)

[Verificação 2: Auditar o Log do Servidor do Gerenciador](#)

[Perguntas mais frequentes](#)

Introdução

Este documento descreve as etapas para identificar e corrigir uma vulnerabilidade de segurança de SD-WAN crítica de acordo com as datas do aviso da PSIRT em 30 de setembro de 2026. A Cisco recomenda enfaticamente a atualização para uma versão de software fixa para corrigir esse problema.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Componentes de arquitetura e controle do Cisco Catalyst SD-WAN (gerenciador, controlador e validador)
- Procedimento de atualização do Cisco Catalyst SD-WAN

- Gerenciamento de casos do Cisco TAC e procedimentos de coleta de tecnologia administrativa

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Para obter informações detalhadas e as atualizações mais recentes, consulte a página oficial do PSIRT Advisory.

Este aviso está disponível neste link:

- [Vulnerabilidade de desvio de autenticação de API do Cisco Catalyst SD-WAN Manager](#) (CVE-2026-76504, CWE-177). Classificação do impacto na segurança: Crítico (Pontuação Base 9,8 do CVSS).

Este defeito é abordado por este aviso PSIRT:

- ID de bug da Cisco [CSCww79570](#)

Este aviso afeta o Cisco Catalyst SD-WAN Manager (vManage).

Visão Geral do Fluxo de Trabalho de Correção



Note: Todos os SD-WAN Managers (vManage) que executam uma versão anterior à primeira versão fixa são vulneráveis e exigem uma atualização imediata. No entanto, nem todos os gerentes Catalyst mostram evidências de comprometimento.

Ação necessária: Colete técnicos administrativos de todos os gerenciadores de SD-WAN do Catalyst, atualize todos para uma versão fixa e abra um caso do Cisco TAC para que o TAC possa verificar seus técnicos administrativos em busca de indicadores de comprometimento.

TAC disponível para:

- Verifique os técnicos de administração que você fornece para obter indicadores de comprometimento
- Fornecer suporte à atualização se você encontrar problemas durante a atualização
- Guiá-lo através de correções adicionais se forem identificados indicadores de

comprometimento

1. Coletar Admin-Techs - Executar admin-tech em todos os Catalyst SD-WAN Managers, incluindo cada nó de um cluster e de uma implantação de Recuperação de Desastres (DR), antes da atualização para garantir que nenhum dado de diagnóstico seja perdido. Selecione as opções Log e Tech. O núcleo não é necessário.
 2. Atualizar para uma versão fixa - Atualizar todos os gerenciadores (vManage) para uma versão fixa de software listada na [tabela Versões fixas de software](#).
-



Note: Não espere pelos resultados da verificação do TAC antes de atualizar. Atualizar para uma versão fixa é a prioridade mais alta e fecha a vulnerabilidade. A verificação do TAC na Etapa 3 determina se alguma ação adicional é necessária após a atualização.

3. Abra um caso de TAC e faça upload de Admin-Techs para verificar indicadores de comprometimento - Abra um caso de TAC da Cisco e faça upload de todos os pacotes de registro de admin-tech coletados na Etapa 1. O TAC verifica os admin-techs para obter indicadores de comprometimento.
 4. Se o comprometimento for identificado, use as orientações do TAC - Se o TAC identificar indicadores de comprometimento em seu ambiente, preencha todas as orientações de correção fornecidas pelo TAC. Se nenhum indicador de comprometimento for encontrado, nenhuma ação além da atualização será necessária.
-

Passo 1: Coletar arquivos de administração técnica de todos os gerentes

obrigatório: Colete arquivos admin-tech de todos os Gerenciadores (vManage) antes da atualização para garantir que nenhum dado de diagnóstico seja perdido. Esses arquivos são usados pelo TAC na Etapa 3 para verificar seu ambiente em busca de indicadores de comprometimento.

Coleção:



Note: Para a geração de admin-tech, selecione as opções Log and Tech (Log e Tecnologia). O núcleo não é necessário.

1. Execute admin-tech em TODOS os gerentes (vManage).
2. Se os gerentes forem executados como um cluster, execute admin-tech em cada membro do cluster.
3. Se você tiver uma implantação de Recuperação de desastres (DR), execute admin-tech em cada Gerenciador no local principal e no local de DR.

[Coletar um Admin-Tech no ambiente SD-WAN e fazer upload para o caso TAC](#)



Note: O TAC analisa esses arquivos para avaliar seu ambiente em busca de indicadores de comprometimento e orientar o caminho de correção apropriado.

Alternativa: Verificação manual (somente se não for possível coletar Admin-Tech)

Para aqueles que não podem compartilhar arquivos admin-tech, as etapas de verificação manual estão disponíveis. Essas etapas fornecem indicadores preliminares que devem ser documentados e compartilhados com o TAC.

Consulte a seção [Etapas de verificação manual](#) no final deste documento para obter os procedimentos detalhados. Documente todas as descobertas e forneça-as ao TAC em seu caso de suporte.

Passo 2: Atualizar para uma versão de software fixo

Depois de coletar os técnicos administrativos na Etapa 1, atualize todos os Gerenciadores (vManage) para uma versão de software fixa.



Importante: Não espere pelos resultados da verificação do TAC antes de atualizar. Atualizar para uma versão fixa é a prioridade mais alta e fecha a vulnerabilidade. A verificação do TAC na Etapa 3 determina se alguma ação adicional é necessária após a atualização.

Selecione a versão apropriada na tabela [Versões de Software Fixo](#) neste documento.



aviso: A atualização deve permanecer na sua versão principal atual. Não atualize para uma versão principal superior sem orientação explícita do TAC.

[Atualize os controladores SD-WAN com o uso da GUI ou CLI do vManage](#)



Note: Se você encontrar algum problema durante a atualização, abra um caso no TAC para obter suporte à atualização.

Passo 3: Abra um caso no TAC e carregue os arquivos do Admin-Tech para verificação

Após a atualização na Etapa 2, abra um caso de suporte do Cisco TAC e carregue os arquivos admin-tech coletados na Etapa 1. O TAC verifica os admin-techs em busca de indicadores de comprometimento.

Ações necessárias:

1. Abra um caso TAC de Gravidade 3 com o CVE-ID "CVE-2026-76504" no título para iniciar o processo de verificação.
2. Carregue TODOS os pacotes de registro admin-tech coletados na Etapa 1 (todos os gerenciadores, incluindo os nós de cluster e DR).
3. Aguarde até que o TAC conclua a verificação e comunique os resultados.



Note: O TAC analisa os arquivos admin-tech e comunica os resultados da verificação. Se nenhum indicador de comprometimento for encontrado, nenhuma ação além da atualização será necessária.

Passo 4: Se o comprometimento for identificado — Diretrizes do TAC

Se o TAC identificar indicadores de comprometimento em seu ambiente, o TAC entrará em contato com você com orientações específicas de correção. Complete todas as instruções fornecidas pelo TAC.

Se nenhum indicador de comprometimento for identificado, a atualização concluída na Etapa 2 será suficiente e nenhuma outra correção será necessária.

Versões de software fixo

Essas versões de software contêm a correção para essa vulnerabilidade. Atualize para a primeira versão fixa da sua versão de treinamento atual.

Software Cisco Catalyst SD-WAN	Primeira versão fixa	Software disponível
Anterior a 20.9 ¹	Migrar para uma versão fixa.	
20.9	20.9.10.1	20.9.10.1 imagens de atualização para

Software Cisco Catalyst SD-WAN	Primeira versão fixa	Software disponível
		vManage
20.12	20.12.8.2	20.12.8.2 imagens de atualização para vManage
20.15	20.15.6.1	20.15.6.1 imagens de atualização para vManage
20.18	20.18.4.1	20.18.4.1 imagens de atualização para vManage
26.1	26.1.2.1	26.1.2.1 imagens de atualização para vManage
26.2	26.2.1	26.2.1 imagens de atualização para vManage

¹ Essas versões chegaram ao fim da manutenção do software. A Cisco incentiva fortemente os clientes a atualizarem para uma versão compatível.

A Cisco Product Security Incident Response Team (PSIRT) valida somente as informações de versão afetadas e fixas que estão documentadas no aviso.



Note: A Cisco também abordou essa vulnerabilidade no Cisco SD-WAN Cloud (Cisco Managed) versão 20.15.605, que é baseada em nuvem. Nenhuma ação do usuário é necessária. Os clientes podem determinar o status atual da correção ou a versão do software usando a função Ajuda na GUI do serviço.

Referências importantes:

- [Matriz de atualização](#)
- [Matriz de compatibilidade do controlador](#)

Anexo: Etapas de verificação manual (somente se a coleta de Admin-Tech não for possível)



Note: A coleta de tecnologia administrativa é o método preferido e recomendado. Use a

verificação manual apenas se você absolutamente não puder coletar e compartilhar arquivos admin-tech. Se você não conseguir coletar arquivos de tecnologia administrativa, use estas etapas manuais para coletar indicadores preliminares para o TAC.



Note:

- Estas etapas fornecem apenas dados preliminares
- A coleta de tecnologia administrativa é altamente preferível para uma avaliação precisa
- Documente suas descobertas e compartilhe-as com o TAC em seu caso de suporte
- O TAC determina a avaliação oficial

Requisitos: Essas etapas devem ser executadas em todos os gerentes (vManage), incluindo cada membro do cluster e cada gerente em um local de recuperação de desastres (DR). Acesse os arquivos de log do vshell (vshe11 da CLI do Gerenciador) e revise os arquivos de log atuais e girados.

Como identificar os indicadores de comprometimento

Este aconselhamento tem dois indicadores de compromisso. Ambos se relacionam a entradas para j_security_check em que um caractere da solicitação é codificado (por exemplo /%6a_security_check), de endereços IP desconhecidos ou não autorizados.



Importante: Os exemplos nesta seção mostram o uso de %6a como o caractere codificado j na solicitação. Este é apenas um exemplo, e a vulnerabilidade permite que qualquer caractere codificado na solicitação seja usado.



Note: Os sistemas Cisco Catalyst SD-WAN Manager que estão expostos à Internet e que têm portas expostas à Internet estão em risco de exposição a comprometimento. Em alguns casos, esses indicadores de comprometimento podem ocorrer durante as operações padrão. Portanto, eles devem ser avaliados em relação à postura normal da rede para identificar e evitar falsos positivos.

Indicador	Arquivo de log	O que isso significa	Verificação
Solicitação j_security_check codificada	/var/log/nms/containers/service_proxy/serviceproxy-access.log*	Um cliente enviou uma	Verificação 1

Indicador	Arquivo de log	O que isso significa	Verificação
recebida		solicitação desse tipo ao gerente.	
Solicitação j_security_check codificada processada para um usuário viptela- reserved-*	/var/log/nms/vmanage-server.log*	O gerente processou uma solicitação desse tipo para um usuário viptela-reserved-* (uma conta de serviço do sistema reservado).	Verificação 2

Verificação 1: Auditoria do Log de Acesso ao Proxy de Serviço

Faça auditoria do arquivo `serviceproxy-access.log`, localizado em `/var/log/nms/containers/service_proxy/serviceproxy-access.log`, para entradas relacionadas a `j_security_check` de endereços IP desconhecidos ou não autorizados, como mostrado neste exemplo:

```
[2026-09-29T23:11:13.948-05:00] "POST /%6a_security_check HTTP/1.1" 200 - 48 0 4 - "10.10.10.47,192.168
```

Determinados arquivos de log no sistema vManage são restritos por trás do acesso raiz e não podem ser acessados diretamente pelos clientes. Para revisar esses logs, os clientes devem gerar um arquivo admin-tech.

Interpretar resultados e documentos do TAC

Se nenhuma dessas entradas for encontrada:

- Nenhum indicador de comprometimento detectado neste log no Gerenciador
- Documente este resultado para seu caso de TAC
- Continue com a Verificação 2 e repita ambas as verificações nos Gerenciadores restantes

Se tais entradas forem encontradas:

- Examine cuidadosamente cada endereço IP de origem mostrado
- Procure entradas de endereços IP desconhecidos ou não autorizados. Verificar se o IP de

origem pertence a uma atividade autorizada em seu ambiente (por exemplo, uma verificação de vulnerabilidade ou um teste de penetração que você executa)

- Se não for possível identificar o IP de origem como legítimo, isso poderá indicar possíveis indicadores de comprometimento
- Documentar todas as descobertas e abrir um caso de TAC imediatamente
- Inclua as entradas de log, os timestamps, os IPs de origem e os códigos de status HTTP no seu caso
- O TAC executa a determinação de avaliação oficial

Verificação 2: Auditar o Log do Servidor do Gerenciador

Faça auditoria do arquivo `vmanage-server.log`, localizado em `/var/log/nms/vmanage-server.log`, para entradas relacionadas a `j_security_check` de endereços IP desconhecidos ou não autorizados, sendo especificamente chamado para usuários que incluem nomes que começam com `viptela-reserved-`, como mostrado neste exemplo:

```
29-Sep-2026 23:11:13,952 CDT [] [vManage-new] [UserUtils] (default task-127462) |default| Request Store
```



Note: As contas de serviço do sistema reservado para `viptela` estão documentadas na seção Autenticação, Autorização e Contabilidade do Guia de Configuração de Sistemas e Interfaces Cisco Catalyst SD-WAN.

Interpretar resultados e documentos do TAC

Se nenhuma dessas entradas for encontrada:

- Nenhum indicador de comprometimento detectado neste log no Gerenciador
- Documente este resultado para seu caso de TAC
- Repetir ambas as verificações nos gerentes restantes

Se tais entradas forem encontradas:

- Isso pode indicar possíveis indicadores de comprometimento
 - Documentar todas as descobertas e abrir um caso de TAC imediatamente
 - Inclua as entradas de registro e os carimbos de data e hora em seu caso, junto com as descobertas da Verificação 1 para o mesmo período de tempo
 - O TAC executa a determinação de avaliação oficial
-

Perguntas mais frequentes

P: Qual é a primeira etapa para lidar com esse consultivo de segurança?

R: Colete arquivos admin-tech de todos os gerentes (vManage) e atualize todos os gerentes para uma versão de software fixa. Após a atualização, abra um caso de TAC e carregue os técnicos de administração para que o TAC possa verificar seu ambiente em busca de indicadores de comprometimento.

P: Quais componentes são afetados por essa consultoria?

R: Somente o Cisco Catalyst SD-WAN Manager (vManage) é afetado.

P: Precisamos atualizar também os controladores, validadores ou roteadores de borda?

R: Não, para não falar sobre esse conselho. Atualize todos os gerenciadores (vManage) para uma versão fixa e use a [Matriz de compatibilidade do controlador](#) para confirmar se a nova versão do gerenciador é compatível com seus outros componentes.

P: Há uma solução alternativa disponível?

R: Não. Não há soluções alternativas para essa vulnerabilidade. Atualize para uma versão fixa.

P: Para qual versão preciso atualizar?

R: Atualize para a primeira versão fixa do seu treinamento de versão atual assim que possível. Consulte a tabela [Versões Fixas de Software](#) neste documento. O TAC confirma a versão apropriada para seu ambiente específico.

P: Já atualizei para uma versão fixa de um aviso de segurança SD-WAN anterior. Preciso atualizar novamente?

R: Sim, a menos que sua versão atual seja igual ou posterior à primeira versão fixa do treinamento na tabela [Versões de software fixo](#). As versões fixas de avisos anteriores não incluem necessariamente a correção dessa vulnerabilidade.

P: Preciso coletar técnicos de administração de todos os gerentes?

R: Yes. O TAC requer arquivos técnicos de administração de cada gerenciador (vManage), incluindo cada membro do cluster e cada gerenciador em um local de recuperação de desastres (DR), para avaliar corretamente seu ambiente.

P: Posso eu mesmo verificar os indicadores de comprometimento?

R: Yes. Se você não puder coletar arquivos admin-tech, use as [Etapas de verificação manual](#) em cada Gerenciador e compartilhe os resultados com o TAC. A coleta de tecnologia administrativa continua sendo o método preferido, e o TAC determina a avaliação oficial.

P: Como o TAC determina se meu sistema foi comprometido?

R: O TAC analisa os arquivos administrativos e técnicos usando ferramentas especializadas para avaliar seu ambiente em busca de indicadores de comprometimento.

P: O que acontece se forem identificados indicadores de comprometimento?

R: O TAC entra em contato com você para discutir as próximas etapas e orientações específicas ao seu ambiente. A Cisco não executa a correção em seu nome — O TAC fornece as orientações necessárias para que você prossiga.

P: Posso iniciar a atualização antes que o TAC analise meus técnicos de administração?

R: Yes. Colete os técnicos administrativos, atualize para uma versão fixa e abra um caso no TAC para que o TAC possa verificar os técnicos administrativos em busca de indicadores de comprometimento.

P: O tempo de inatividade é esperado durante a correção?

R: O impacto depende da sua arquitetura de implantação e do caminho de correção. O TAC fornece orientação sobre como minimizar o impacto do serviço durante o processo.

P: Tenho uma sobreposição de SD-WAN hospedada na nuvem. Quais são minhas opções de atualização?

R: Para sobreposições hospedadas na nuvem, os clientes têm duas opções:

1. Verifique se o ambiente está agendado para uma atualização automática navegando até SSP > Detalhes de Sobreposição > Alterar Janelas.
2. Se você não quiser esperar pela atualização agendada, terá duas opções:
 - Atualize você mesmo usando os guias de atualização disponíveis neste documento.
 - Abra um caso TAC de espera para a janela de manutenção de sua preferência. O TAC está disponível para ajudá-lo se você encontrar dificuldades com a atualização.

P: Somos uma sobreposição hospedada pela Cisco. Precisamos revisar alguma regra de acesso à SSP?

R: Todos os clientes hospedados pela Cisco são aconselhados a revisar suas próprias regras de entrada permitidas no SSP > Detalhes de sobreposição > Permitir regras de entrada e garantir que somente os prefixos necessários do seu lado sejam permitidos. Essas regras são apenas para acesso de gerenciamento e não se aplicam a roteadores de borda.

P: O Cisco TAC oferece análise forense ou serviços de investigação para essa vulnerabilidade?

R: O Cisco TAC pode ajudar os clientes verificando os Indicadores de comprometimento (IoCs) relacionados a essa vulnerabilidade. No entanto, o TAC não realiza análises forenses detalhadas ou investigações de incidentes. Para um trabalho de computação forense abrangente ou investigações de segurança detalhadas, recomendamos que os clientes envolvam a empresa de terceiros de resposta a incidentes (IR) de sua preferência.

P: Quais são as melhores práticas gerais ou maneiras de reduzir as vulnerabilidades da minha sobreposição de SD-WAN?

R: Consulte o [Guia de Proteção de SD-WAN do Cisco Catalyst](#) para obter as melhores práticas e recomendações para reduzir as vulnerabilidades na sobreposição de SD-WAN.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.