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

Contents

Introdução

Este documento descreve as etapas para identificar e lidar com vulnerabilidades de segurança críticas na SD-WAN com base nos avisos da PSIRT de 4 de junho de 2026.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Componentes de arquitetura e controle do Cisco Catalyst SD-WAN (vManage, vSmart, vBond)
- 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.

Essas recomendações estão disponíveis nos seguintes links:

- Vulnerabilidade de escalação de privilégios autenticados do Cisco Catalyst SD-WAN Manager

Esses defeitos são abordados por estes avisos PSIRT:

- ID de bug Cisco CSCwu18563

Visão Geral do Fluxo de Trabalho de Correção

Este aviso descreve uma vulnerabilidade de escalação de privilégio no SD-WAN Manager que exige privilégios de administrador de rede para explorar.

De acordo com o aviso, os caminhos conhecidos para que um invasor remoto não autenticado obtenha esses privilégios são a exploração de CVE-2026-20182 (cisco-sa-sdwan-rpa2-v69WY2SW) ou CVE-2026-20127 (cisco-sa-sdwan-rpa-EHchtZk).

Se seus componentes de controle tiverem sido atualizados para uma versão fixa para esses dois avisos, e a Cisco não tiver identificado nenhum indicador de comprometimento (IoCs) em potencial nos arquivos admin-tech fornecidos para os eventos anteriores, os caminhos de exploração não autenticados conhecidos para essa nova vulnerabilidade serão reduzidos nesses dispositivos específicos, com base nos arquivos analisados.

Isso não elimina a exposição quando um invasor mantém credenciais de netadmin válidas. A Cisco ainda não lançou uma correção de software para essa vulnerabilidade e não há soluções alternativas disponíveis; à medida que se tornarem disponíveis, serão dadas mais orientações.

Ação necessária:Abra um caso no Cisco TAC para tratar desse aviso de segurança.

TAC disponível para:

- Avaliar seu ambiente em busca de indicadores de comprometimento
- Guiá-lo pelo caminho de remediação apropriado com base na avaliação
- Fornecer orientações sobre as próximas etapas necessárias caso sejam identificados indicadores de comprometimento

1. Coletar Admin-Techs- Executar admin-tech em todos os componentes de controle (vSmart, vManage, vBond). Os técnicos de administração do vSmart não devem ser executados simultaneamente — execute-os um de cada vez. Todos os outros podem ser coletados em qualquer ordem. Selecione as opções Log e Tech. O núcleo não é necessário.
2. Caso de TAC aberto - Entre em contato com o TAC da Cisco e forneça todos os pacotes de log de Admin-tech do componente de controle.
3. Avaliação do TAC- Realizar uma avaliação preliminar de indicadores de comprometimento no seu ambiente e o TAC executa uma avaliação preliminar de indicadores de comprometimento no seu ambiente.
4. Execute a correção- Conclua o processo específico fornecido pelo TAC, se necessário.

Passo 1: Coletar arquivos de administração técnica de todos os componentes de controle

obrigatório: Colete arquivos técnicos de administração de todos os componentes de controle antes de qualquer atualização ou alteração de configuração para que os dados de diagnóstico e qualquer indicador de comprometimento (IoCs) em potencial sejam preservados. Esses arquivos são usados pelo TAC na Etapa 3 para analisar seu ambiente.

Coleção: para geração de admin-tech, selecione as opções Log e Tech. O núcleo não é necessário.

1. Execute o admin-tech em TODOS os controladores (vSmarts) — não execute-os simultaneamente; coletar um de cada vez
2. Execute admin-tech em TODOS os gerentes (vManages)
3. Execute admin-tech em TODOS os Validadores (vBonds)

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 relacionados a essa recomendação. A análise deste aviso concentra-se em uma entrada de log específica que não distingue entre uso legítimo e mal-intencionado; é necessária uma revisão manual pelo TAC.

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

Para clientes que não podem compartilhar arquivos admin-tech, uma etapa de verificação manual está disponível. Esta etapa fornece um indicador preliminar que deve ser documentado e compartilhado com o TAC.

Consulte a seção Etapas de verificação manual no final deste documento para obter o procedimento detalhado. Documente todas as descobertas e forneça-as ao TAC em seu caso de suporte.

Passo 2: Abra um caso no TAC e carregue arquivos administrativos

Depois de coletar os técnicos administrativos na Etapa 1, abra um caso de suporte do Cisco TAC e carregue os arquivos técnicos de administração coletados. O TAC analisa os técnicos administrativos para obter indicadores de comprometimento associados a essa recomendação.

Ações necessárias:

1. Abra um caso de TAC de Gravidade 3 com "CVE-2026-20245" e o ID de aviso `cisco-sa-sdwan-privesc-4uxFrdzx` no título para iniciar a análise.
2. Carregue TODOS os pacotes de registro admin-tech coletados na Etapa 1 (Controladores, Gerentes e Validadores).
3. Aguarde até que o TAC conclua a análise e comunique os resultados.

Note: A Cisco não lançou uma correção de software para essa vulnerabilidade e não há soluções alternativas disponíveis. A análise do TAC na Etapa 3 ajuda a determinar se algum indicador de comprometimento está presente nos arquivos admin-tech fornecidos por você. Outras orientações serão seguidas à medida que forem disponibilizadas pela engenharia.

Passo 3: Avaliação do TAC

O TAC executa uma análise preliminar dos arquivos admin-tech que você carregou na Etapa 2 e os avalia quanto a indicadores de comprometimento associados a essa recomendação.

Para esta recomendação, a análise se concentra em uma entrada de log específica em `/var/log/scripts.log` em cada gerente (vManage). Como o comando subjacente é legítimo e o registro não distingue entre uso legítimo e mal-intencionado, qualquer entrada correspondente requer revisão manual pelo TAC em relação à postura operacional normal do cliente antes de ser tratada como um indicador confirmado.

Possíveis resultados da análise do TAC:

- Nenhuma entrada de log correspondente identificada — com base nos arquivos admin-tech

revisados, nenhum indicador associado a esta recomendação foi observado. Não é necessária nenhuma outra ação específica para este aviso no momento. O resultado é limitado aos arquivos admin-tech recebidos e pode ser limitado pelo período de retenção de log em cada dispositivo.

- Correspondência das entradas de registro identificadas — O TAC envolverá o cliente com etapas adicionais de revisão. Como a Cisco não lançou uma correção de software para este aviso, a atualização sozinha não resolve essa vulnerabilidade. A orientação do TAC para cenários de comprometimento confirmado está documentada nos artigos relacionados da TechZone mencionados na Etapa 4.

Note: De acordo com a recomendação, a exploração dessa vulnerabilidade requer privilégios netadmin, que um invasor não autenticado pode obter apenas por meio de credenciais válidas ou da exploração de CVE-2026-20182 ou CVE-2026-20127. Se os componentes de controle tiverem sido atualizados para uma versão fixa para ambos os consultivos e nenhum indicador de comprometimento tiver sido identificado para os eventos anteriores, os caminhos de exploração não autenticados conhecidos para essa nova vulnerabilidade serão atenuados nesses dispositivos específicos, com base nos arquivos revisados.

Passo 4: Se forem identificados indicadores de comprometimento — siga as orientações do TAC

Se o TAC identificar indicadores de comprometimento associados a essa recomendação no seu ambiente, o TAC entrará em contato com você para obter orientações específicas. Complete todas as instruções fornecidas pelo TAC.

Se nenhum indicador de comprometimento for identificado para esta recomendação, nenhuma outra ação específica para esta recomendação será necessária no momento, com base nos arquivos técnicos de administração revisados.

Importante: A Cisco não lançou uma correção de software para este aviso e não há soluções alternativas disponíveis. Como a exploração dessa vulnerabilidade requer privilégios netadmin obtidos por meio de CVE-2026-20182 ou CVE-2026-20127, os clientes devem garantir que a correção desses avisos anteriores esteja completa. Consulte os documentos correspondentes para o fluxo de remediação estabelecido:

Considerações

Após a conclusão de uma remediação bem-sucedida, e com base nos requisitos de garantia de

segurança específicos de cada cliente, os clientes podem avaliar e agir nas seguintes atividades de higiene. Essas atividades se aplicam independentemente da opção de remediação selecionada. São gerenciados pelo cliente; A Cisco não os dirige ou executa em nome do cliente.

- Revisão de todas as contas de usuário locais
- Rotação de credenciais
- Rotação de segredos presentes nas configurações do dispositivo, por exemplo (lista não exaustiva):
    - Credenciais para contas de usuário locais
    - Strings de comunidade SNMP
    - Chaves secretas TACACS
    - Certificados e chaves pré-compartilhadas de VPN
    - Chaves SSH confiáveis
- Revisão dos modelos de configuração

Dispositivos de borda da rede — suspeita de comprometimento

A Cisco não recomenda um caminho de remediação específico; a seleção de uma opção de remediação é do cliente. Como uma nota informativa para clientes que estão avaliando seu ambiente: em caso de suspeita de comprometimento de um dispositivo de borda pelo cliente, a redefinição e a reintegração de fábrica do(s) dispositivo(s) de borda afetado(s) é uma ação gerenciada pelo cliente que o cliente pode querer levar em conta ao fazer sua seleção. A decisão de prosseguir com essa abordagem e qual opção selecionar é do cliente.

O comando apropriado para executar uma redefinição de fábrica segura é:

```
factory-reset all secure 3-pass
```

Versões de software fixo

⚠ Importante: No momento da publicação deste documento, a Cisco não lançou uma correção de software que aborde o CVE-2026-20245. De acordo com o aviso, a Cisco planeja abordar essa vulnerabilidade no Cisco Catalyst SD-WAN Manager em uma versão futura. Não há soluções alternativas. Esta seção será atualizada quando o software fixo estiver disponível.

Como a exploração dessa vulnerabilidade requer privilégios de netadmin que um invasor não autenticado pode obter apenas por meio do CVE-2026-20182 ou do CVE-2026-20127, os clientes são incentivados a garantir que seus componentes de controle executem uma versão fixa para esses avisos anteriores. As versões fixas para esses avisos estão documentadas no documento de 14 de maio de 2026 do Aviso de Segurança da SD-WAN e no documento correspondente do

TechZone:

- Vulnerabilidade de desvio de autenticação do controlador Cisco Catalyst SD-WAN (14 de maio de 2026)
- (Tabela de versões fixas de software)

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 coleção Admin-tech é o método preferido. Use apenas a etapa de verificação manual abaixo se os arquivos técnicos de administração não puderem ser coletados e compartilhados com o TAC. O resultado desta etapa manual é preliminar; documentar as descobertas e compartilhá-las com o TAC, que realiza a avaliação oficial.

Note: Para esta recomendação, a verificação manual consiste em uma única verificação de log direcionada. A entrada de log pesquisada é gerada por um comando legítimo e o log sozinho não distingue entre uso legítimo e mal-intencionado. Qualquer entrada correspondente deve ser analisada em relação à postura operacional normal do cliente antes de ser tratada como um indicador potencial. Se uma entrada correspondente não puder ser reconciliada com as operações normais, documente a descoberta e compartilhe-a com o TAC.

Verificação: Verifique `scripts.log` em cada Gerenciador (vManage) para Entradas de Carregamento da Lista de Locatários

De acordo com o aviso da PSIRT, os clientes são incentivados a auditar o arquivo `scripts.log`, localizado em `/var/log/`, para entradas semelhantes ao exemplo a seguir:

```
Apr 15 09:44:57 vmanage vScript: Tenant list upload per vsmart serial number: /usr/bin/vconfd_script_up
```

Passo 1: Acesse o vshell em cada Gerenciador (vManage) e pesquise o arquivo de log

Na CLI do vManage, acesse vshell e execute:

```
vs
zgrep "vconfd_script_upload_tenant_list.sh" /var/log/scripts.log*
```

Repita a verificação em cada vManage na implantação (incluindo todos os membros do cluster e qualquer vManage emparelhado com DR).

Passo 2: Interpretar resultados e documentos do TAC

Se NENHUMA entrada correspondente for retornada:

- Nenhum indicador de comprometimento associado a este aviso foi observado no arquivo de log neste dispositivo.
- Documente este resultado para seu caso TAC (inclua o nome de host do dispositivo e a data/intervalo dos arquivos de log pesquisados).
- Continue a verificação nos gerentes restantes.

Se entradas correspondentes forem retornadas:

- Cada entrada correspondente deve ser analisada em relação à postura operacional normal do cliente. O comando subjacente (carregamento de lista de locatários) é legítimo e pode aparecer durante operações de rotina.
- Para cada entrada correspondente, capture o timestamp, a linha de registro completa e o caminho do arquivo referenciado após o `-cli path`.
- Se uma entrada correspondente não puder ser reconciliada com uma operação conhecida e legítima, isso pode ser um indicador de comprometimento. Documente a descoberta e forneça-a ao TAC para revisão.
- Documente todas as descobertas e abra um caso de TAC. Inclua as entradas de registro correspondentes e a saída do comando source no seu caso.
- O TAC realiza a avaliação oficial. Se a avaliação identificar indicadores de comprometimento, siga o fluxo descrito nos documentos relacionados do TechZone: e guias de correção.

Perguntas mais freqüentes

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

R: Colete arquivos técnicos de administração de todos os componentes de controle (vSmart, vManage, vBond) antes de qualquer atualização ou alteração de configuração para preservar dados de diagnóstico e quaisquer indicadores potenciais de comprometimento. Em seguida, abra um caso do Cisco TAC e faça upload dos técnicos administrativos para que o TAC possa analisá-los.

P: A Cisco lançou uma correção de software para essa vulnerabilidade?

R: Não no momento da publicação deste documento. De acordo com a consultoria, a Cisco

planeja abordar essa vulnerabilidade no Cisco Catalyst SD-WAN Manager em uma versão futura. Não há soluções alternativas. Este documento será atualizado quando uma versão fixa se tornar disponível.

P: Se não há correção, por que a Cisco recomenda alguma ação agora?

R: A exploração dessa vulnerabilidade requer privilégios netadmin. De acordo com a recomendação, um invasor não autenticado pode obter esses privilégios somente por meio de credenciais válidas ou por meio da exploração de CVE-2026-20182 ou CVE-2026-20127. Garantir que os componentes de controle sejam atualizados para as versões fixas desses avisos anteriores aborda os caminhos não autenticados conhecidos para obter os privilégios necessários para explorar essa vulnerabilidade. A análise admin-tech na Etapa 3 ajuda a determinar se algum indicador de comprometimento está presente nos arquivos revisados.

P: Preciso coletar técnicos de administração de todos os componentes do controle?

R: Yes. O TAC exige arquivos técnicos de administração de todos os controladores (vSmart, coletados um de cada vez), todos os gerentes (vManage) e todos os validadores (vBond) para executar a análise.

P: Como o TAC determina se meu sistema tem indicadores de comprometimento associados a essa consultoria?

R: O TAC analisa os arquivos admin-tech e procura a entrada de log específica descrita no aviso PSIRT em `/var/log/scripts.log` em cada Gerenciador. O comando subjacente é legítimo; qualquer entrada correspondente deve ser analisada em relação à sua postura operacional normal antes de ser tratada como um indicador potencial. O TAC executa essa revisão.

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

R: O TAC entra em contato com você com orientações específicas. Como não há correções de software disponíveis no momento para este aviso, a atualização sozinha não resolve um comprometimento confirmado. As orientações do TAC seguem o fluxo documentado nos artigos relacionados da TechZone para os avisos de maio de 2026 e fevereiro de 2026.

P: Os roteadores de borda (Cisco IOS XE) são afetados por essa recomendação?

R: Este aviso afeta o Cisco Catalyst SD-WAN Manager. De acordo com a consultoria, a Cisco observou casos limitados em que a exploração dessa vulnerabilidade resultou em uma alteração de configuração enviada para dispositivos de borda; os clientes são incentivados a verificar a configuração de seus dispositivos de borda.

P: Quais tipos de implantação são afetados?

R: De acordo com a consultoria, essa vulnerabilidade afeta todos os tipos de implantação do Cisco Catalyst SD-WAN Manager, independentemente da configuração do dispositivo, incluindo a implantação no local, Cisco SD-WAN Cloud-Pro, Cisco SD-WAN Cloud (Cisco Managed) e Cisco SD-WAN for Government (FedRAMP).

P: Já atualizei para os consultivos de maio de 2026 e fevereiro de 2026 e não foram identificados indicadores de compromisso para esses eventos. Estou exposto a essa nova vulnerabilidade?

R: Se seus componentes de controle estiverem executando uma versão fixa para CVE-2026-20182 e CVE-2026-20127 e nenhum indicador de comprometimento tiver sido identificado para esses eventos anteriores nos arquivos admin-tech revisados, os caminhos de exploração não autenticados conhecidos para essa nova vulnerabilidade serão mitigados nesses dispositivos específicos, com base nos arquivos revisados. Isso não elimina a exposição quando um invasor mantém credenciais netadmin válidas.

P: Posso fazer a verificação sozinho em vez de esperar pelo TAC?

R: Os clientes que não podem compartilhar técnicos administrativos podem executar a etapa de verificação manual descrita no Apêndice. O resultado é preliminar; documentar as descobertas e compartilhá-las com o TAC, que realiza a avaliação oficial.

P: Quais são as práticas recomendadas gerais para fortalecer minha sobreposição de SD-WAN?

R: Consulte o Guia de Proteção de SD-WAN do Cisco Catalyst para obter as melhores práticas.

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

R: O TAC da Cisco pode ajudar os clientes revisando os arquivos técnicos de administração para obter os indicadores de comprometimento documentados no consultivo da PSIRT. O Cisco TAC não realiza análises forenses detalhadas ou investigações de incidentes. Para um trabalho de computação forense abrangente ou investigações de segurança detalhadas, os clientes são incentivados a envolver sua empresa de resposta a incidentes (IR) de terceiros preferida.

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.