Consultoria de segurança do Catalyst SD-WAN de correção - fevereiro 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 componentes de controle](#)

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

[Passo 2: Abra um caso no TAC e carregue arquivos administrativos](#)

[Passo 3: Avaliação do TAC](#)

[Passo 4: Executar correção (guiado pelo TAC)](#)

- [Caminho A: Nenhum indicador de comprometimento encontrado — Atualização](#)
- [Caminho B: Indicadores de comprometimento identificados — guiados por PSIRT](#)

[Versões de software fixo](#)

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

- [Verificação 1: Verificar Logons SSH Não Autorizados em Logs Auth](#)
- [Verificação 2: Verificar Conexões de Peer Não Autorizadas em Syslogs de Controlador](#)

[Perguntas mais freqüentes](#)

Introdução

Este documento descreve as etapas para identificar e corrigir vulnerabilidades de segurança críticas na SD-WAN com base nos avisos da PSIRT de 25 de fevereiro 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:

- Vulnerabilidades do Cisco Catalyst SD-WAN
- Vulnerabilidade de desvio de autenticação do controlador Cisco Catalyst SD-WAN

Esses defeitos são abordados por estes avisos PSIRT:

- ID de bug da Cisco CSCws52722
- ID de bug da Cisco CSCws33583
- ID de bug da Cisco CSCws33584
- ID de bug da Cisco CSCws33585
- ID de bug da Cisco CSCws33586
- ID de bug da Cisco CSCws33587
- ID de bug da Cisco CSCws93470

Visão Geral do Fluxo de Trabalho de Correção

Note: Todas as implantações de SD-WAN são vulneráveis e exigem ação imediata. No entanto, nem todos os sistemas mostram evidências de comprometimento.

Ação necessária: Abra um caso do 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
- Trabalhar com a equipe PSIRT se forem identificados indicadores de comprometimento
- Fornecer orientação e suporte para atualização se nenhum indicador de comprometimento for detectado

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 - O TAC avalia seu ambiente para indicadores de comprometimento
4. Executar correção - concluir o processo específico fornecido pelo TAC

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

obrigatório: Reúna arquivos de admin-tech de todos os componentes de controle antes de abrir o caso do TAC. Isso é essencial para o TAC avaliar seu ambiente.

Coleção:

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

Note: Os técnicos administrativos do vSmart não devem ser executados simultaneamente — colete-os um de cada vez. Os técnicos de administração para gerentes e validadores podem ser coletados em qualquer ordem.

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: Abra um caso no TAC e carregue arquivos administrativos

Depois de coletar todos os arquivos admin-tech da Etapa 1, abra um caso de suporte do Cisco TAC.

Ações necessárias:

1. Abra um caso de TAC com o nível de gravidade adequado ao impacto nos negócios
2. Carregue TODOS os pacotes de registro admin-tech coletados na Etapa 1 (Controladores, Gerentes e Validadores)
3. Consulte as recomendações da PSIRT
4. Aguarde a avaliação e a orientação do TAC

⚠ Caution: O TAC determina o status do seu sistema e recomenda as próximas etapas apropriadas.

Não tente executar outras etapas sem a orientação do TAC

Passo 3: Avaliação do TAC

O TAC analisa os arquivos admin-tech carregados e determina o status do sistema.

Durante esse período:

- Aguardar uma avaliação oficial do TAC antes de tomar qualquer medida
- O TAC entra em contato com você para informar suas descobertas e as próximas etapas

---

Passo 4: Executar correção (guiado pelo TAC)

O TAC orienta você pelo processo de correção apropriado com base na avaliação. Complete todas as instruções fornecidas pelo TAC.

Caminho A: Nenhum indicador de comprometimento encontrado — Atualização

Se o TAC confirmar que não há evidências de comprometimento, atualize para a versão fixa do software. Selecione a versão apropriada na tabela Versões de Software Fixo neste documento e consulte o guia de atualização vinculado nesta seção.

---

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

Caminho B: Indicadores de comprometimento identificados — guiados por PSIRT

Se o TAC confirmar a presença de indicadores de comprometimento, eles envolverão a equipe PSIRT para desenvolver uma estratégia de correção personalizada específica para o seu ambiente. Preencha todas as orientações fornecidas pelo TAC e pela PSIRT.

Versões de software fixo

Estas versões de software contêm correções para as vulnerabilidades identificadas:

Aplica-se às versões atuais	Versão Fixa	Software disponível
20.3, 20.6, 20.9	20.9.8.2 *	20.9.8.2 imagens de atualização para vManage, vSmart e vBond
20.10, 20.11, 20.12.5 e anteriores em 20.12	20.12.5.3	20.12.5.3 imagens de atualização para vManage, vSmart e vBond
20.12.6	20.12.6.1	20.12.6.1 imagens de atualização para vManage, vSmart e vBond
20.13, 20.14, 20.15.x	20.15.4.2	20.15.4.2 imagens de atualização para vManage, vSmart e vBond
20.16, 20.17, 20.18.x	20.18.2.1	20.18.2.1 imagens de atualização para vManage, vSmart e vBond

---

Note: Para clientes em CDCS (Cisco-Hosted Cluster), 20.15.405 também é uma versão fixa. Isso se aplica especificamente à implantação de cluster hospedado pela Cisco e é tratado separadamente do caminho de atualização padrão.

---

* Se você estiver na versão 20.9 ou anterior: O software fixo para a sua versão (20.9.8.2) está disponível em 27/2. A Cisco recomenda que você permaneça na sua versão principal atual e aguarde a versão 20.9.8.2 em vez de atualizar para uma versão principal mais alta (20.12, 20.15, 20.18). Se você estiver atualmente em uma versão inferior a 20.9, aguarde 20.9.8.2 para atualizar lá. Continue a trabalhar com o TAC e verifique novamente em 27/02 para obter o link de software disponível.

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: Estas etapas devem ser executadas em todos os componentes do controle.

Verificação 1: Verificar Logons SSH Não Autorizados em Logs Auth

Passo 1: Identificar IPs válidos do sistema vManage

Acesse cada controlador vSmart e execute:

```
west-vsmart# show control connections | inc "vmanage|PEER|IP"
```

Saída de exemplo:

```
                                                PEER
      PEER  PEER  PEER            SITE       DOMAIN  PRIV    PEER                                    PUB
INDEX TYPE  PROT  SYSTEM IP       ID         ID      PRIVATE IP                           PORT    PUBLIC I
-------------------------------------------------------------------------------------------------------
0     vmanage dtls 10.1.0.18     101018     0       10.1.10.18                           12346   10.1.10.1
```

Passo 2: Criar sequência de expressão regular (somente vBond e vSmart)

Combine todos os IPs do sistema da Etapa 1 em um padrão regex OR:

```
system-ip1|system-ip2|...|system-ipn
```

Passo 2b: Etapa adicional para sistemas vManage

Se você estiver executando esses comandos no próprio vManage, anexe o IP do localhost (127.0.0.1), o IP do sistema local, todos os IPs de cluster e o IP da interface de transporte da VPN 0 ao regex:

```
system-ip1|system-ip2|...|system-ipn|127.0.0.1|
```

Para localizar o IP do sistema vManage local, use:

```
show control local-properties
```

Para localizar o IP da interface de transporte da VPN 0 e o IP do cluster, use:

```
show interface | tab
```

Passo 3: Executar Comando de Verificação

Execute este comando, substituindo REGEX pela sua string regex da Etapa 2:

```
west-vsmart# vs
west-vsmart:~$ zgrep "Accepted publickey for vmanage-admin from " /var/log/auth.log* | grep -vE "\s(REG
```

Note: Este comando filtra logs de autenticação para mostrar apenas logons vmanage-admin de fontes inesperadas. Logons legítimos devem ser originados apenas de IPs relacionados ao vManage.

Passo 4: Interpretar resultados e documentos do TAC

Se NENHUMA saída for exibida:

- Nenhum indicador de comprometimento detectado neste dispositivo
- Documente este resultado para seu caso de TAC
- Continuar a avaliação dos controladores restantes

Se as linhas de log forem impressas:

- Examine cuidadosamente cada endereço IP mostrado
- Verifique se o IP não está relacionado à infraestrutura do vManage (IP do cluster, IP antigo do sistema ou similar)
- Se não for possível identificar o IP de origem como legítimo, isso poderá indicar possíveis indicadores de comprometimento
- A entrada de registro mostra um carimbo de data/hora e um endereço IP de origem
- Documentar todas as descobertas e abrir um caso de TAC imediatamente
- Inclua as entradas de registro, carimbos de data/hora e IPs de origem no seu caso
- O TAC executa a determinação de avaliação oficial

Verificação 2: Verificar Conexões de Peer Não Autorizadas em Syslogs de Controlador

Esse comando extrai todos os pares peer-type e peer-system-ip dos arquivos syslog do controlador e os exibe como uma lista para você revisar. Ele não sinaliza automaticamente entradas suspeitas — você deve inspecionar a saída e determinar se cada IP de sistema de peer é uma parte legítima e conhecida de sua infraestrutura de SD-WAN. Execute isso em todos os componentes de controle (Controladores, Gerenciadores e Validadores).

Passo 1: Execute o comando em cada componente de controle:

Primeiro, acesse vshell e navegue até o diretório de log:

```
vs
cd /var/log
```

Em seguida, execute este comando:

```
awk '{
  match($0, /peer-type:([a-zA-Z0-9]+)[^ ]* peer-system-ip:([0-9.:]+)/, arr);
  if(arr[1] && arr[2]) print "(" arr[1] ", " arr[2] ")";
}' vsyslog* | sort | uniq
```

Passo 2: Interpretar resultados e documentos do TAC

Se a saída mostrar apenas IPs de sistema vManage/vSmart/vBond conhecidos:

- Nenhum indicador de comprometimento detectado nesta verificação
- Documente este resultado para seu caso de TAC
- Continuar a avaliação dos componentes de controle restantes

Se a saída contiver IPs de sistemas pares não reconhecidos:

- Examine cuidadosamente cada endereço IP e tipo de peer mostrado
- Verifique se o IP não está relacionado à sua infraestrutura conhecida do plano de controle da SD-WAN
- 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 a saída completa do comando com pares peer-type e peer-system-ip no seu caso
- O TAC executa a determinação de avaliação oficial

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 e abra um caso no TAC para carregar os arquivos. O TAC avalia seu ambiente e fornece orientação sobre as próximas etapas.

P. Para qual versão devo atualizar? A. Atualize para a versão fixa mais próxima o mais cedo possível.

P: Preciso coletar técnicos de administração de todos os componentes do controle? R: Sim, 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 avaliar corretamente seu ambiente.

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

P: Como posso saber qual versão de software fixa usar?

R: Consulte a tabela Versões Fixas de Software neste documento. O TAC confirma a versão apropriada para seu ambiente específico.

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

R: Não, aguarde até que o TAC conclua sua avaliação e forneça orientação antes de tentar qualquer ação corretiva.

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: As correções de PSIRT estão incluídas na próxima versão 20.15.5 e em outras versões futuras?

R: Sim, as correções serão incluídas em 20.15.5 e em outras versões futuras. No entanto, a atualização para atenuar as vulnerabilidades descritas neste documento deve ser priorizada IMEDIATAMENTE. (Não espere!)

P: Todos os controladores precisam ser atualizados caso nenhum indicador de comprometimento seja encontrado?

R: Sim, todos os componentes de controle da SD-WAN (vManage, vSmart e vBond) devem ser atualizados para uma versão de software fixa. A atualização de apenas um subconjunto de controladores não é suficiente.

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 ajudará se você encontrar dificuldades com a atualização.

P: Precisamos atualizar os roteadores de borda também?

R: Os dispositivos Cisco IOS XE não são afetados por este aviso.

P: Somos uma sobreposição hospedada pela Cisco. Precisamos corrigir alguma ACL ou executar uma ação no SSP?

R: Todos os clientes hospedados pela Cisco são aconselhados a revisar suas próprias regras de entrada permitidas vistas no SSP 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. Revise-os em SSP > Detalhes de sobreposição > Permitir regras de entrada. Observe que a porta 22, 830 sempre foi bloqueada por padrão no provisionamento do dia 0 pela Cisco de fora para os controladores hospedados na nuvem.

P:Estamos em CDCS/Locatário compartilhado. Para qual versão nós vamos ser atualizados?

R: Com base na versão atual, os clusters de Locatário Compartilhado ou CDCS estão atualmente no cronograma para serem atualizados OU já foram atualizados para as versões fixas. Estas são as versões fixas compartilhadas de locatário e CDCS:

1. Clusters Early Adoter => 20.18.2.1 (isso é realmente o mesmo que a versão padrão)

2. Clusters de versão recomendados => 20.15.405 (versão específica do CDCS com correções PSIRT)

Os clientes de CDCS não precisam tomar nenhuma ação eficaz para lidar com essa PSIRT.

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.