

Verificar se há negrito nos artigos já existentes

Contents

[Introdução](#)

[Referências — Documentação do Cisco SD-WAN CVE-2026-20182](#)

[E-mails](#)

[Sherlock 1 - Entrada - Solicitação de atualização e arquivos de administração técnica](#)

[Sherlock 2 - Resultado - sem IoCs observados \(por arquivo\)](#)

[Sherlock 3 - Lembrete - Arquivos administrativos ausentes](#)

[TAC 1 - Investigação - Revisão adicional necessária \(suspeita-se de IoC\)](#)

[TAC 2 - Resultado - Nenhum IoCs encontrado \(confirmado pelo engenheiro\)](#)

[TAC 3 - Validação - Confirmar propriedade de IP em sobreposição](#)

[TAC 4 - Resultado - Falso Positivo Eliminado](#)

[TAC 5 - Crítico - IoC identificado. Agendar revisão da chamada](#)

[TAC 6 - Resultado - Duplicar IoC \(Fechar e Redirecionar\)](#)

[TAC 7 - Correção - Opções de acompanhamento \(pós-chamada\)](#)

[TAC 8 - Correção - Opções atualizadas para malhas comprometidas \(Opção 2 - Acompanhamento\)](#)

[TAC 17 - Descoberta revertida - Antes não havia IoC, agora a IoC foi identificada \(CVE-2026-20182\)](#)

[CloudOps 1 - Pró-ativo - IoC detectado em verificação de nuvem, necessidade de administração técnica para validar](#)

[E-mails para WAVE 2A para clientes AFETADOS ANTERIORMENTE que ainda não preencheram as Opções A, B OU C. \(As Opções 1 e 2 precisam ser refeitas\)](#)

[Modelo do TAC 9 para nenhum IOC para PSIRT2a/eles reconstruíram \(PREVIOUSLY IMPACTED\)](#)

[Modelo do TAC 10 para sim IOC para PSIRT2a/eles reconstruíram \(PREVIOUSLY IMPACTED\)](#)

[Modelo do TAC 11 para nenhum IOC para PSIRT2a/eles não reconstruíram \(IMPACTADO ANTERIORMENTE\)](#)

[Modelo do TAC 12 para sim IOC para PSIRT2a/eles não reconstruíram \(PREVIOUSLY IMPACTED\)](#)

[E-mails para WAVE 2A para NOVOS clientes \(não afetados anteriormente\)](#)

[Modelo do TAC 13 para IOC inexistente / Nenhuma versão fixa disponível \(WAVE 2a — Aguarde a correção\)](#)

[Modelo do TAC 14 para IOC/versão fixa não disponível \(WAVE 2a — Atualize agora\)](#)

[Modelo do TAC 15 para IOC identificado/versão fixa disponível \(WAVE 2a — Atualização urgente\)](#)

[Modelo do TAC 16 para IOC identificado / Nenhuma versão fixa disponível \(WAVE 2a — Harden & Await Fix\)](#)

Introdução

Este documento centraliza os modelos de e-mail do cliente aprovados usados durante a triagem e a correção de casos relacionados à vulnerabilidade de desvio de autenticação do controlador de

SD-WAN do Cisco Catalyst. Os modelos são divididos por remetente - Sherlock (trocas de casos automatizadas que coletam dados técnicos de administração e retornam resultados preliminares de IoC) e engenheiro do TAC (acompanhamentos conduzidos por humanos para investigação, validação e orientação de correção).

Referências — Documentação do Cisco SD-WAN CVE-2026-20182

Lista mestre de todos os documentos da Cisco mencionados nos modelos de e-mail acima. A numeração é unificada — sobrescritos por e-mail (por exemplo, ^[2]) aponte para os itens desta lista.

1. Guia de fortalecimento da SD-WAN da Cisco — <https://sec.cloudapps.cisco.com/security/center/resources/Cisco-Catalyst-SD-WAN-HardeningGuide>
2. Consultoria de segurança oficial (cisco-sa-sdwan-mltnps2-JxpWm7R) — <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>
3. Guia de correção do TAC — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225842-remediate-catalyst-sd-wan-security.html#toc-hld--1516256622>
4. Guia de atualização do Cisco SD-WAN — <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>
5. Guia de coleta de SD-WAN Admin-Tech da Cisco — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/216954-how-to-collect-an-admin-tech-in-an-sd-wa.html>
6. Segunda Consultoria de Segurança (cisco-sa-sdwan-rpa2-v69WY2SW) — <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>
7. Inicie a atualização do Catalyst SD-WAN — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

E-mails

Sherlock 1 - Entrada - Solicitação de atualização e arquivos de administração técnica

Caso de uso

Alcance inicial quando um caso de TAC é aberto para CVE-2026-20182 para aconselhar a coleta de dados técnicos administrativos de e, em seguida, atualizar todos os componentes de controle SD-WAN.

Assunto

Mensagem

Caro cliente,

Obrigado por entrar em contato com o Cisco Technical Assistance Center (TAC).

Em relação à vulnerabilidade associada ao **CVE-2026-20182**, analise o [aviso oficial de segurança](#)[1] para obter todos os detalhes, bem como o Guia de correção do TAC[2].

Nosso objetivo principal é ajudar a proteger seu ambiente. Priorize **o planejamento e a execução da atualização** como a etapa mais importante na mitigação desse risco. Se você ainda não agendou esta atualização, faça-o imediatamente.

Recursos de atualização: Consulte o seguinte documento oficial da Cisco para obter instruções detalhadas sobre como executar a atualização: [Guia de atualização do Cisco SD-WAN](#)[3]

Para permitir a avaliação inicial do seu ambiente para qualquer indicador de comprometimento (IoCs) potencial relacionado ao CVE-2026-20182, você deve executar uma coleta de admin-tech *antes* da atualização. Siga esta ordem de operações:

- 1. Coletar arquivos administrativos:** Gere os logs admin-tech de todos os componentes de controle da SD-WAN antes da atualização para garantir que nenhum dado de diagnóstico seja perdido. Certifique-se de selecionar **"Logs"** e **"Tech"** ao gerar esses arquivos.
 - **vSmarts (controladores):** Colete um de cada vez, não simultaneamente.
 - **vBonds (Validadores):** Coletar de todos os nós.
 - **Gerente (vManage):** Coletar de todos os nós no cluster (DR ativo e standby).
- 2. Executar atualização:** Atualizar todos os componentes de controle SD-WAN (vManage, vSmart, vBond) para uma versão de software fixa listada no consultivo. Não espere pela análise do log admin-tech antes de começar a atualização, pois a atualização fecha a vulnerabilidade imediatamente.
- 3. Carregar no caso TAC:** Quando a atualização estiver concluída, carregue os arquivos coletados anteriormente para o caso TAC existente simultaneamente, se possível. Em seguida, nossa equipe realizará uma verificação desses registros para avaliar seu ambiente em busca de Indicadores de comprometimento (IoCs).

Recursos e suporte:

Para obter mais detalhes e instruções passo a passo sobre como gerar, bem como enviar com segurança, seus arquivos

admin-tech, consulte este guia: [Guia de coleta de SD-WAN Admin-Tech da Cisco](#)^[4].

Se você tiver uma assinatura do BCS/LCS, entre em contato com seu Cisco NCE ou Gerente de entrega para obter orientação adicional sobre o processo de atualização ou as próximas etapas.

A privacidade e a segurança dos seus dados continuam sendo a nossa principal prioridade. Todas as informações fornecidas serão tratadas de acordo com as políticas de privacidade e segurança da Cisco.

Você receberá um e-mail de confirmação automático para **CADA** arquivo carregado com êxito para o caso; certifique-se de revisar essas notificações.

Agradecemos sua pronta cooperação para proteger sua infraestrutura.

Links:

[1] [Consultoria oficial de segurança](#)

[2] [Guia de correção do TAC](#)

[3] [Guia de atualização do Cisco SD-WAN](#)

[4] [Guia de coleta do administrador da Cisco SD-WAN](#)

Atenciosamente,

Abrir no Outlook

① Use o download .eml abaixo. Substitua todos os *[espaços reservados entre colchetes]* antes de enviar.

✉ Abrir Outlook (assunto apenas)

↓ Baixar .eml Template

Sherlock 2 - Resultado - sem IoCs observados (por arquivo)

Caso de uso

Enviado depois que a análise admin-tech não mostra nenhum indicador de comprometimento observado para um arquivo carregado específico. Enviado uma vez por arquivo processado.

Assunto

Atualizar: Resultados da análise para o componente SD-WAN [Inserir nome do arquivo] - CVE-2026-20182

Mensagem

Caro cliente,

Obrigado por sua paciência.

Concluimos a análise do arquivo admin-tech [Inserir nome do arquivo]. Nesse arquivo, não identificamos nenhum indicador de comprometimento relacionado ao CVE-2026-20182 para esse dispositivo específico.

Observe que a quantidade de dados de registro que você recuperou e forneceu à Cisco para esta revisão pode ter sido limitada pelo período de retenção de registro configurado de acordo com o **Guia de proteção de SD-WAN da Cisco**[1] .

Importante: Próximas etapas e fechamento do caso:

1. **Aguardar Todos os Resultados:** Observe que os resultados neste e-mail podem ser parciais. Analisaremos cada arquivo conforme for fornecido. Aguarde até receber a confirmação de todos os arquivos carregados antes de considerar a avaliação concluída.
2. **Prioridade de atualização:** Embora as varreduras preliminares de registros administrativos e técnicos não tenham identificado indicadores de comprometimento (IoCs), a vulnerabilidade subjacente pode permanecer. Para implantações Cisco Cloud-Pro e Cisco On-Prem, se ainda não o fez, priorize a atualização completa de seus componentes de controle SD-WAN assim que possível.
 - Cisco Cloud (também conhecido como: As malhas do cliente do SaaS são atualizadas automaticamente pela Cisco como parte do serviço gerenciado. Nenhuma ação necessária.
3. **Encerramento do caso:** Depois de receber os resultados de "nenhum IoC observado" para todos os arquivos carregados E (se aplicável) de ter concluído com êxito o upgrade de software em seu ambiente, você pode considerar este caso resolvido e continuar com os procedimentos de fechamento padrão.

Atualizar recursos (se aplicável): Consulte o seguinte documento oficial da Cisco para obter instruções detalhadas sobre como executar a atualização para o Cisco Cloud-Pro e Cisco On-Prem: Guia de atualização do Cisco SD-WAN

Uma visão geral de alto nível do processo de upgrade inclui:

1. Carregar as imagens de software apropriadas no repositório do Gerenciador (vManage).
2. Atualização sequencial dos controladores, começando com Manager (vManage), seguido por Validator (vBond) e Controller (vSmart).
3. Ativando as novas versões de software e validando a funcionalidade do sistema.

Continuaremos monitorando seu caso. Se não recebermos resposta dentro de 10 dias úteis após fornecermos todos os resultados com base nos arquivos que recebemos de você, presumiremos que não será necessária mais assistência e prosseguiremos com os procedimentos normais de fechamento de caso do TAC. Se precisar de ajuda a qualquer momento, entre em contato conosco.

Atenciosamente,

① Substitua todos os [espaços reservados entre colchetes] antes de enviar.

✉ Abrir Outlook (assunto apenas)

↓ Baixar .eml Template

Sherlock 3 - Lembrete - Arquivos administrativos ausentes

Caso de uso

Acompanhamento automatizado quando os arquivos admin-tech enviados não corresponderem ao número de componentes de controle SD-WAN encontrados nos logs.

Assunto

Lembrete: Arquivos administrativos necessários para a avaliação do CVE-2026-20182 ausentes

Mensagem

Caro cliente,

Ainda não temos técnicos de administração nos componentes de controle da SD-WAN, portanto nosso sistema não pode avaliar nenhum indicador de comprometimento nos registros de tecnologia de administração. Para iniciar a avaliação CVE-2026-20182, devemos receber arquivos técnicos de administração de TODOS os controladores (vSmarts), validadores (vBonds) e gerentes (vManage), incluindo todos os nós do Manager (vManage), se estiverem em cluster.

Próximas etapas:

Carregue os arquivos admin-tech restantes assim que for possível.

Atenciosamente,

Abrir no Outlook

① Substitua todos os [espaços reservados entre colchetes] antes de enviar.

✉ Abrir Outlook (com corpo)

↓ Baixar .eml Template

TAC 1 - Investigação - Revisão adicional necessária (suspeita-se de IoC)

Caso de uso

Enviado pelo engenheiro do TAC quando a automação encontra registros indicando um possível comprometimento e é necessária investigação humana.

Assunto

Nº da SS - Necessidade de investigação adicional

Mensagem

Caro cliente,

Meu nome é {your_name} e eu aceitei seu caso. Agradecemos sua cooperação contínua com o Cisco Technical Assistance Center (TAC).

Após uma análise preliminar dos arquivos admin-tech que você forneceu de **seus componentes de controle SD-WAN**, identificamos que é necessária uma investigação adicional do TAC para concluir nossa análise. Para ajudar a garantir uma resolução completa e precisa, trabalharei com você nas próximas etapas.

Esteja certo de que estamos comprometidos em apoiá-lo durante as próximas etapas e forneceremos orientações claras para lidar com a situação de forma eficaz.

Priorize o planejamento e a execução da atualização como a etapa mais importante para atenuar esse risco. Se você ainda não agendou esta atualização, faça-o imediatamente.

Em caso de dúvidas ou se precisar de ajuda, entre em contato com o engenheiro do TAC.

Agradecemos sua atenção e colaboração.

Atenciosamente,

Abrir no Outlook

① Substitua todos os **[espaços reservados entre colchetes]** antes de enviar.

✉ Abrir Outlook (com corpo)

↓ Baixar .eml Template

TAC 2 - Resultado - Nenhum IoCs encontrado (confirmado pelo engenheiro)

Caso de uso

Enviado pelo engenheiro do TAC depois que a automação não encontrou nenhum indicador de comprometimento e o engenheiro confirmou o resultado.

Assunto

Atualizar: Revisão do TAC concluída - Nenhum IoCs encontrado para CVE-2026-20182 - Caso [SR #]

Mensagem

Olá, [Nome do cliente],

Sou o engenheiro do TAC da Cisco designado para o seu caso [Número da SS].

Após executar uma verificação preliminar dos arquivos admin-tech fornecidos por você a partir dos componentes de controle da SD-WAN, não encontramos entradas de registro consistentes com os indicadores de comprometimento descritos nas Recomendações de Segurança da SD-WAN da Cisco:

- **Vulnerabilidade de desvio de autenticação do controlador Cisco Catalyst SD-WAN [1]**
- **Vulnerabilidades do Cisco Catalyst SD-WAN Manager [2]**

No entanto, você deve continuar a atualizar todos os componentes de controle da SD-WAN para <inserir versão>. Estas são as etapas para continuar com a atualização:

- **Inicie a atualização do Catalyst SD-WAN [3]**
- **Guia de atualização do Cisco SD-WAN[4]**

Observe que a Cisco não pode avaliar registros de dispositivos de borda devido à natureza dinâmica do endereçamento IP na Internet e à nossa falta de conhecimento dos endereços IP esperados dos dispositivos de borda na rede de um cliente. Os clientes são incentivados a seguir as orientações de validação de eventos de troca de tráfego (Peering Event Validation Guidance) anotadas no Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability Security Advisory para concluir manualmente esta etapa. Os clientes também são incentivados a concluir as etapas adicionais de detecção relacionadas à validação do evento de troca de tráfego (peering), conforme descrito no Security Advisory for CVE-2026-20182.

Links

[1] Vulnerabilidade de desvio de autenticação do controlador Cisco Catalyst SD-WAN -

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>

[2] Vulnerabilidades do Cisco Catalyst SD-WAN Manager -

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>

[3] Inicie a atualização do Catalyst SD-WAN — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

[4] Guia de atualização do Cisco SD-WAN — <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>

Atenciosamente,

Abrir no Outlook

① Substitua todos os **[espaços reservados entre colchetes]** antes de enviar.

✉ Abrir Outlook (assunto apenas)

↓ Baixar .eml Template

TAC 3 - Validação - Confirmar propriedade de IP em sobreposição

Caso de uso

Enviado pelo engenheiro do TAC para perguntar ao cliente se os endereços IP específicos exibidos durante a análise de log são ou faziam parte de sua infraestrutura de sobreposição de SD-WAN.

Assunto

[Nº da SS] - Validação de Endereço IP Necessária

Mensagem

Prezado(a) [Nome do cliente],

Meu nome é [Seu nome] e sou o engenheiro do Cisco TAC designado para o seu caso.

Como parte de nossa análise contínua dos arquivos de administração técnica que você forneceu de seus componentes de controle da SD-WAN, precisamos de sua ajuda para validar se os seguintes endereços IP são ou eram anteriormente parte de sua infraestrutura de sobreposição da SD-WAN:

Endereços IP em questão:

- [Endereço IP 1]
- [Endereço IP 2]

Para nos ajudar a concluir nossa avaliação, confirme:

1. Este endereço IP está atualmente associado a algum componente na sua sobreposição de SD-WAN (por exemplo, vManage, vSmart, vBond ou dispositivo de borda)?
2. Esse endereço IP foi usado anteriormente por algum componente de controle da SD-WAN que tenha sido desativado

ou cujo IP tenha sido alterado?

3. Este IP está associado a um local de recuperação de desastres (DR) ou a qualquer outra infraestrutura relacionada à sua implantação de SD-WAN?

Sua resposta imediata nos permitirá continuar nossa análise e fornecer as próximas etapas apropriadas.

Em caso de dúvidas, não hesite em entrar em contato conosco.

Atenciosamente,

Abrir no Outlook

① Substitua todos os [espaços reservados entre colchetes] antes de enviar.

✉ Abrir Outlook (com corpo)

↓ Baixar .eml Template

TAC 4 - Resultado - Falso Positivo Eliminado

Caso de uso

Enviado pelo engenheiro do TAC após uma revisão manual determinar que o IoC inicial sinalizado pela verificação automatizada era um falso positivo.

Assunto

Atualizar: Revisão técnica para CVE-2026-20182 - Caso [Número do caso]

Mensagem

Caro cliente,

Obrigado por sua paciência enquanto nossa equipe de engenharia conduzia uma revisão manual dos arquivos de administração-tecnologia que você forneceu a partir de seus componentes de controle SD-WAN.

Após uma investigação minuciosa, determinamos que o indicador inicial de comprometimento (IoC) sinalizado pelo nosso processo de verificação automatizada era um falso positivo, ou seja, nossa avaliação é que os IoCs não são válidos.

Importante: Embora este alerta específico tenha sido eliminado, observe que a vulnerabilidade associada ao [CVE-2026-20182](#)^[1] requer uma atualização de software para ajudar a garantir a segurança e a integridade a longo prazo da malha SD-WAN.

Se você ainda não concluiu a atualização: Priorize a atualização completa dos componentes de controle da SD-WAN assim que possível. A atualização é a única maneira de remediar efetivamente essa vulnerabilidade. Consulte o [Guia de atualização do Cisco SD-WAN](#)[2] para obter instruções detalhadas.

Se você já tiver concluído a atualização: Como confirmamos esta descoberta como um falso positivo e você já executou a correção de software, nenhuma ação adicional é necessária. Você pode considerar este caso resolvido e continuar com os procedimentos de fechamento padrão.

Agradecemos sua diligência em priorizar a segurança de sua infraestrutura. Se você tiver mais alguma dúvida ou precisar de assistência adicional, não hesite em entrar em contato conosco.

Atenciosamente,
Cisco Technical Assistance Center (TAC)

Links:

[1] [Consultoria oficial de segurança](#)

[2] [Guia de atualização do Cisco SD-WAN](#)

Abrir no Outlook

ⓘ Substitua todos os *[espaços reservados entre colchetes]* antes de enviar.

✉ Abrir Outlook (assunto apenas)

⬇ Baixar .eml Template

TAC 5 - Crítico - IoC identificado, Agendar revisão da chamada

Caso de uso

Enviado pelo engenheiro do TAC quando os indicadores potenciais de comprometimento foram confirmados e uma chamada urgente ao cliente é necessária para discutir as descobertas e as próximas etapas.

Assunto

URGENTE: Resultados da análise para CVE-2026-20182 - Indicador de comprometimento identificado

Mensagem

Caro cliente,

Obrigado por sua paciência enquanto analisávamos os arquivos admin-tech fornecidos para seus componentes de controle SD-WAN.

Após nossa revisão técnica, identificamos possíveis Indicadores de Comprometimento (IoCs) relacionados ao CVE-2026-20182.

Dada a natureza destas constatações, é fundamental que discutamos os pormenores técnicos e as próximas etapas recomendadas o mais rapidamente possível. Gostaríamos de agendar uma chamada com sua equipe para analisar as descobertas específicas e discutir a correção apropriada.

Próximas etapas:

- **Agendar uma reunião:** Informe-nos sobre sua disponibilidade para uma breve ligação dentro das próximas [por exemplo, 4-8 horas] para analisar essas descobertas.
- **Atualizar Componentes de Controle SDWAN:** Atualize seu gerenciador, controlador e validador de SDWAN para uma versão fixa o mais rápido possível.

Nosso objetivo principal é ajudá-lo a proteger seu ambiente e mitigar quaisquer riscos potenciais. Agradecemos sua atenção imediata a este assunto e esperamos coordenar com você.

Atenciosamente,

Abrir no Outlook

① Substitua todos os *[espaços reservados entre colchetes]* antes de enviar.

✉ Abrir Outlook (com corpo)

⬇ Baixar .eml Template

TAC 6 - Resultado - Duplicar IoC (Fechar e Redirecionar)

Caso de uso

Enviado pelo engenheiro do TAC quando a análise da IoC confirma as descobertas que correspondem a um SR anterior para o mesmo cliente/ambiente. O caso atual é encerrado e o cliente é redirecionado para o SR original, onde a orientação para remediação já foi fornecida.

Assunto

Atualizar: Revisão técnica para CVE-2026-20182 - Caso [Nº da SR] (IoC duplicado confirmado)

Mensagem

Caro cliente,

Obrigado por sua paciência enquanto analisávamos os arquivos admin-tech fornecidos para seus componentes de controle SD-WAN. Determinamos que os indicadores iniciais de comprometimento (IoC) sinalizados por nosso processo de digitalização são os mesmos que já foram comunicados em **[Nº SR original]**. Conforme discutido anteriormente, recomendamos uma atualização urgente e a continuação de um dos dois caminhos de remediação descritos no [Guia de remediação do TAC](#)[2] para proteger seu ambiente o mais rápido possível. Consulte o [aviso de segurança oficial para CVE-2026-20182](#)[1] para obter detalhes completos.

Vou encerrar este caso. Use o **[Nº SR original]** para solicitar mais orientação ou suporte técnico em relação à sua atualização ou correção.

Atenciosamente,

[Seu nome]

Links:

[1] [Consultoria oficial de segurança](#)

[2] [Guia de correção do TAC](#)

Abrir no Outlook

① Substitua todos os *[espaços reservados entre colchetes]* antes de enviar.

✉ Abrir Outlook (com corpo)

⬇ Baixar .eml Template

TAC 7 - Correção - Opções de acompanhamento (pós-chamada)

Caso de uso

Enviado após a chamada de revisão da IoC para recapitular os caminhos de correção discutidos. O cliente escolhe a opção A (Reimplantação com reinicialização contínua), a opção B (Reimplantação com transição forçada) ou a opção C (Recriação total do sistema).

Assunto

Acompanhamento: Opções de correção para CVE-2026-20182

Mensagem

Caro cliente,

Obrigado pelo tempo que dedicou à discussão dos resultados de nossa análise recente. Conforme discutimos na chamada anterior, recomendamos que você prossiga com um dos seguintes caminhos de correção para proteger seu

ambiente.

Opção A: Reimplantação com reinicialização deslocável. Prioriza a continuidade operacional, evitando o tempo de inatividade da rede, embora apresente um risco residual de persistência de ameaças durante o processo de transição.

Descrição: Envolve a reimplantação do controlador, mais a chave SSH e a rotação de certificado. Os componentes do controlador existentes são conectados durante a migração por meio do vManage para implantar a nova malha e, em seguida, cada um é removido assim que o dispositivo é migrado.

Opção B: Redistribuição com transição forçada. Fornece um nível mais alto de garantia de segurança. Como os novos controladores nunca se conectam a controladores antigos, há um isolamento completo. Devido a isso, há um impacto nas operações gerais da rede, pois todos os dispositivos precisam restabelecer a conectividade e trocar informações de rota/conectividade. O tempo de paralisação dependerá do número de locais, do número de prefixos trocados etc.

Descrição: Envolve a reimplantação do controlador mais a chave SSH e a rotação de certificado, mas os componentes antigos do controlador são isolados da nova malha durante a reimplantação.

Opção C: Reconstrução completa do sistema. Oferece o mais alto nível de garantia de segurança, estabelecendo uma linha de base limpa, embora seja a abordagem mais complexa e apresente um risco maior de instabilidade relacionada à configuração durante a reconstrução. Essa é uma opção demorada e exige experiência na reconstrução dos bancos de dados de modelos e políticas.

Próximas etapas:

- Discuta essas opções internamente e informe-nos sobre o caminho que pretende seguir. Depois que você decidir, podemos fornecer mais orientação ou suporte técnico para ajudá-lo na fase de execução.

Estamos aqui para apoiá-lo em todo este processo. Informe-nos se você tiver alguma dúvida em relação a essas opções.

Atenciosamente,

Cisco Technical Assistance Center (TAC)

NOTE: A opção 1 foi a atualização. O cenário considerado para esta atualização já foi executado.

Abrir no Outlook

① Use o download .eml abaixo. Substitua todos os *[espaços reservados entre colchetes]* antes de enviar.

✉ Abrir Outlook (assunto apenas)

↓ Baixar .eml Template

TAC 8 - Correção - Opções atualizadas para malhas comprometidas (Opção 2 - Acompanhamento)

Caso de uso

Notificar os clientes cujas malhas de SD-WAN foram comprometidas e perseguidas anteriormente Opção 2 e cujas malhas são consideradas como permanecendo em risco de persistência do fator de ameaça. Os clientes que reconstruíram sua malha comprometida (e não confiaram em um backup/configDB existente) não são considerados em risco e não receberão essa comunicação. Esta comunicação será enviada por TBD.

Assunto

Ação urgente necessária: Correção de vulnerabilidade crítica da infraestrutura de SD-WAN

Mensagem

Caro cliente,

Estamos fornecendo uma atualização importante para a correção da malha SD-WAN, conforme mencionado em [SR#] e nos avisos de segurança comunicados anteriormente. Esta atualização é específica para as malhas nas quais os registros fornecidos mostraram evidência de Indicadores de Comprometimento (IOCs).

Embora você tenha selecionado anteriormente um plano de reparo com base na Opção 2 — incorporando uma atualização de software, reimplantação de controlador e rotação de chaves SSH — nossa análise do cenário de ameaças continuou a evoluir. As novas informações técnicas sobre a exploração destas vulnerabilidades indicam que são fortemente exigidas medidas adicionais para reduzir o risco de persistência e ajudar a garantir a integridade da cadeia de certificados de confiança.

Ação exigida:

Atualizamos as estratégias de correção recomendadas para fornecer uma defesa mais abrangente, incluindo rotação adicional de certificados raiz.

Informamos que as correções exigirão atividades de manutenção adicionais, que podem incluir tempo de inatividade planejado da rede.

Como nossa prioridade é a segurança e a integridade da sua rede, desenvolvemos três opções de correção distintas. Cada opção abaixo fornece um equilíbrio entre o impacto operacional e a garantia de segurança para sua consideração. Como sua postura interna de risco é única, a Cisco não pode recomendar um caminho específico.

Opção A: Reimplantação com reinicialização deslocável. Prioriza a continuidade operacional, evitando o tempo de inatividade da rede, embora apresente um risco residual de persistência de ameaças durante o processo de transição.

Descrição: Envolve a reimplantação do controlador, mais a chave SSH e a rotação de certificado. Os componentes do controlador existentes são conectados durante a migração por meio do vManage para implantar a nova malha e, em seguida, cada um é removido assim que o dispositivo é migrado.

Opção B: Redistribuição com transição forçada. Fornece um nível mais alto de garantia de segurança. Como os novos controladores nunca se conectam a controladores antigos, há um isolamento completo. Devido a isso, há um impacto nas operações gerais da rede, pois todos os dispositivos precisam restabelecer a conectividade e trocar informações de rota/conectividade. O tempo de paralisação dependerá do número de locais, do número de prefixos trocados etc.

Descrição: Envolve a reimplantação do controlador mais a chave SSH e a rotação de certificado, mas os componentes antigos do controlador são isolados da nova malha durante a reimplantação.

Opção C: Reconstrução completa do sistema. Oferece o mais alto nível de garantia de segurança, estabelecendo uma linha de base limpa, embora seja a abordagem mais complexa e apresente um risco maior de instabilidade relacionada à configuração durante a reconstrução. Essa é uma opção demorada e exige experiência na reconstrução dos bancos de dados de modelos e políticas.

Assim que sua equipe tiver analisado essas opções e identificado a abordagem que melhor se alinha com seus padrões de gerenciamento de riscos, entre em contato conosco respondendo a esta mensagem. Ao recebermos sua seleção, coordenaremos a janela de manutenção e iniciaremos os preparativos técnicos necessários para a execução.

Agradecemos o seu foco contínuo na manutenção de uma infraestrutura de rede segura. Informe-nos se você precisar de mais esclarecimentos técnicos abrindo uma Solicitação de Serviço (SR) com nosso Centro de Assistência Técnica (TAC).

Atenciosamente,
Cisco

Abrir no Outlook

① Use o download .eml abaixo. Substitua todos os **[espaços reservados entre colchetes]** antes de enviar.

✉ Abrir Outlook (assunto apenas)

↓ Baixar .eml Template

TAC 17 - Descoberta revertida - Antes não havia IoC, agora a IoC foi identificada (CVE-2026-20182)

Caso de uso

Enviado para clientes **informados anteriormente de que não foram encontrados indicadores de comprometimento (IoCs)**, mas para os quais uma **revisão interna subsequente** dos logs de administração técnica identificou desde então **IoCs** relacionados ao CVE-2026-20182. Comunica a descoberta revisada e fornece as três opções de correção (Opção A, B ou C).

Assunto

Atualização importante: Avaliação da IoC revisada para CVE-2026-20182 - Indicadores de comprometimento já

Mensagem

Caro cliente,

Agradecemos sua cooperação contínua com o Cisco Technical Assistance Center (TAC) em relação ao CVE-2026-20182 sob solicitação de serviço [SR#].

Em nossa correspondência anterior, informamos que nossa análise dos arquivos de tecnologia administrativa fornecidos pelos componentes de controle da SD-WAN não identificou nenhum indicador de comprometimento (IoCs) relacionado a essa consultoria. Como parte de nosso compromisso contínuo com a sua segurança, realizamos desde então uma revisão interna de rotina dos dados de log adicionais de admin-tech associados à malha da sua organização.

Essa revisão subsequente identificou Indicadores de comprometimento (IoCs) que não foram apresentados durante a avaliação inicial. Estamos trabalhando com você para resolver esses problemas. Esses IoCs indicam uma atividade potencialmente suspeita na malha da sua organização que justifica ações de correção.

Reconhecemos que isso revisa o resultado comunicado anteriormente a você e queremos garantir que você tenha uma imagem clara e precisa do seu ambiente para que a correção apropriada possa ser feita.

Ação exigida:

Informamos que as correções exigirão atividades de manutenção adicionais, que podem incluir tempo de inatividade planejado da rede.

Como nossa prioridade é a segurança e a integridade da sua rede, desenvolvemos três opções de correção distintas. Cada opção abaixo fornece um equilíbrio entre o impacto operacional e a garantia de segurança para sua consideração. Como sua postura interna de risco é única, a Cisco não pode recomendar um caminho específico.

Opção A: Reimplantação com reinicialização deslocável. Prioriza a continuidade operacional, evitando o tempo de inatividade da rede, embora apresente um risco residual de persistência de ameaças durante o processo de transição.

Descrição: Envolve a reimplantação do controlador, mais a chave SSH e a rotação de certificado. Os componentes do controlador existentes são conectados durante a migração por meio do vManage para implantar a nova malha e, em seguida, cada um é removido assim que o dispositivo é migrado.

Opção B: Redistribuição com transição forçada. Fornece um nível mais alto de garantia de segurança. Como os novos controladores nunca se conectam a controladores antigos, há um isolamento completo. Devido a isso, há um impacto nas operações gerais da rede, pois todos os dispositivos precisam restabelecer a conectividade e trocar informações de rota/conectividade. O tempo de paralisação dependerá do número de locais, do número de prefixos trocados etc.

Descrição: Envolve a reimplantação do controlador mais a chave SSH e a rotação de certificado, mas os componentes

antigos do controlador são isolados da nova malha durante a reimplantação.

Opção C: Reconstrução completa do sistema. Oferece o mais alto nível de garantia de segurança, estabelecendo uma linha de base limpa, embora seja a abordagem mais complexa e apresente um risco maior de instabilidade relacionada à configuração durante a reconstrução. Essa é uma opção demorada e exige experiência na reconstrução dos bancos de dados de modelos e políticas.

Assim que sua equipe tiver analisado essas opções e identificado a abordagem que melhor se alinha com seus padrões de gerenciamento de riscos, entre em contato conosco respondendo a esta mensagem. Ao recebermos sua seleção, coordenaremos a janela de manutenção e iniciaremos os preparativos técnicos necessários para a execução.

Agradecemos o seu foco contínuo na manutenção de uma infraestrutura de rede segura. Informe-nos se você precisar de mais esclarecimentos técnicos respondendo a este e-mail ou através da Solicitação de Serviço (SR) existente com nosso Centro de Assistência Técnica (TAC).

Atenciosamente,
Cisco

Abrir no Outlook

① Use o download .eml abaixo. Substitua todos os *[espaços reservados entre colchetes]* antes de enviar.

✉ Abrir Outlook (assunto apenas)

↓ Baixar .eml Template

CloudOps 1 - Pró-ativo - IoC detectado em verificação de nuvem, necessidade de administração técnica para validar

Caso de uso

Enviado de forma proativa quando uma verificação de segurança do Cisco CloudOps de uma malha SD-WAN hospedada na nuvem apresenta possíveis Indicadores de Comprometimento (IoCs). Um SR é aberto em nome do cliente e o cliente é solicitado a anexar arquivos admin-tech para que a descoberta possa ser validada por meio de uma análise de log completa.

Assunto

Ação exigida: Arquivos de administração técnica necessários para validar os resultados da verificação de segurança - SR [SR#]

Mensagem

Caro cliente,

Como parte de nosso compromisso contínuo de proteger e monitorar a integridade das ofertas da Cisco, a Cisco concluiu recentemente uma verificação de segurança de malhas SD-WAN hospedadas na nuvem. Esta ação foi tomada em resposta a uma preocupação de segurança relatada. A varredura identificou uma atividade potencialmente suspeita na malha da sua organização que justifica uma análise mais detalhada.

Estamos solicitando sua ajuda para anexar arquivos de administração técnica a esta Solicitação de Serviço (SR), que foi aberta em seu nome, para que possamos validar esta descoberta e concluir nossa investigação.

Para habilitar uma análise completa, colete e carregue arquivos admin-tech de todos os componentes de controle da SD-WAN. Certifique-se de selecionar "**Logs**" e "**Tech**" ao gerar estes arquivos:

- **vSmarts (controladores):** Colete um de cada vez, não simultaneamente.
- **vBonds (Validadores):** Coletar de todos os nós.
- **Gerente (vManage):** Coletar de todos os nós no cluster (DR ativo e standby).

Para obter instruções detalhadas e passo a passo sobre como gerar e enviar com segurança seus arquivos admin-tech, consulte este guia: [Guia de coleta de SD-WAN Admin-Tech da Cisco](#)^[1].

Assim que recebermos os arquivos solicitados, nossa equipe os analisará para confirmar se a atividade observada representa um indicador de comprometimento genuíno e o aconselhará sobre as próximas etapas apropriadas.

Agradecemos o seu foco contínuo na manutenção de uma infraestrutura de rede segura. Informe-nos se você precisar de mais esclarecimentos técnicos respondendo a esta Solicitação de Serviço (SR).

Atenciosamente,
Cisco

Links:

[1] [Guia de coleta do administrador da Cisco SD-WAN](#)

Abrir no Outlook

① Use o download .eml abaixo. Substitua todos os *[espaços reservados entre colchetes]* antes de enviar.

✉ Abrir Outlook (assunto apenas)

↓ Baixar .eml Template

E-mails para WAVE 2A para clientes AFETADOS ANTERIORMENTE que ainda não preencheram as Opções A, B OU C. (As Opções 1 e 2 precisam ser refeitas)

Modelo do TAC 9 para nenhum IOC para PSIRT2a/eles reconstruíram (PREVIOUSLY IMPACTED)

Caso de uso

Enviado a clientes cujos registros SD-WAN não mostraram **nenhum indicador de comprometimento (IoCs)** relacionado à consultoria PSIRT2a E que **reconstruíram anteriormente** sua malha. Fornece orientações atualizadas sobre correções com três opções (acompanhamento da Opção 2).

Assunto

Ação urgente necessária: Correção de vulnerabilidade crítica da infraestrutura SD-WAN - SR [SR#]

Mensagem

Caro cliente,

Obrigado por entrar em contato com o Cisco Technical Assistance Center (TAC) com relação aos avisos SD-WAN PSIRT recentes em Solicitação de serviço [SR#].

Depois de analisar os registros e as informações fornecidas pela malha da SD-WAN, nossa análise não identificou nenhum indicador de comprometimento (IOCs) associado à recomendação de vulnerabilidade da SD-WAN de 5 de junho de 2026. Além disso, entendemos que seu ambiente passou anteriormente por uma reconstrução como parte dos esforços de remediação relacionados a avisos anteriores.

Gostaríamos de compartilhar uma atualização importante sobre as diretrizes de remediação recomendadas para estruturas SD-WAN considerando informações recém-identificadas relacionadas a essas vulnerabilidades.

Estamos fornecendo uma atualização importante para a correção da malha SD-WAN, conforme mencionado em [SR#] e nos avisos de segurança comunicados anteriormente.

Embora você tenha selecionado anteriormente um plano de reparo com base na Opção 2 — incorporando uma atualização de software, reimplantação de controlador e rotação de chaves SSH — nossa análise do cenário de ameaças continuou a evoluir. As novas informações técnicas sobre a exploração destas vulnerabilidades indicam que são fortemente exigidas medidas adicionais para reduzir o risco de persistência e ajudar a garantir a integridade da cadeia de certificados de confiança.

Ação exigida:

Atualizamos as estratégias de correção recomendadas para fornecer uma defesa mais abrangente, incluindo rotação adicional de certificados raiz.

Informamos que as correções exigirão atividades de manutenção adicionais, que podem incluir tempo de inatividade planejado da rede. Como nossa prioridade é a segurança e a integridade da sua rede, desenvolvemos três opções de correção distintas. Cada opção abaixo fornece um equilíbrio entre o impacto operacional e a garantia de segurança para

sua consideração. Como sua postura interna de risco é única, a Cisco não pode recomendar um caminho específico.

Opção A: Reimplantação com reinicialização deslocável. Prioriza a continuidade operacional, evitando o tempo de inatividade da rede, embora apresente um risco residual de persistência de ameaças durante o processo de transição.

Descrição: Envolve a reimplantação do controlador, mais a chave SSH e a rotação de certificado. Os componentes do controlador existentes são conectados durante a migração por meio do vManage para implantar a nova malha e, em seguida, cada um é removido assim que o dispositivo é migrado.

Opção B: Redistribuição com transição forçada. Fornece um nível mais alto de garantia de segurança. Como os novos controladores nunca se conectam a controladores antigos, há um isolamento completo. Devido a isso, há um impacto nas operações gerais da rede, pois todos os dispositivos precisam restabelecer a conectividade e trocar informações de rota/conectividade. O tempo de paralisação dependerá do número de locais, do número de prefixos trocados etc.

Descrição: Envolve a reimplantação do controlador mais a chave SSH e a rotação de certificado, mas os componentes antigos do controlador são isolados da nova malha durante a reimplantação.

Opção C: Reconstrução completa do sistema. Oferece o mais alto nível de garantia de segurança, estabelecendo uma linha de base limpa, embora seja a abordagem mais complexa e apresente um risco maior de instabilidade relacionada à configuração durante a reconstrução. Essa é uma opção demorada e exige experiência na reconstrução dos bancos de dados de modelos e políticas.

Assim que sua equipe tiver analisado essas opções e identificado a abordagem que melhor se alinha com seus padrões de gerenciamento de riscos, entre em contato conosco respondendo a esta mensagem. Ao recebermos sua seleção, coordenaremos a janela de manutenção e iniciaremos os preparativos técnicos necessários para a execução.

Agradecemos o seu foco contínuo na manutenção de uma infraestrutura de rede segura. Informe-nos se você precisar de mais esclarecimentos técnicos respondendo a este e-mail ou através da solicitação de serviço existente.

Atenciosamente,
Cisco

Abrir no Outlook

① Use o download .eml abaixo. Substitua todos os **[espaços reservados entre colchetes]** antes de enviar.

✉ Abrir Outlook (assunto apenas)

↓ Baixar .eml Template

Modelo do TAC 10 para sim IOC para PSIRT2a/eles fizeram a reconstrução
(PREVIOUSLY IMPACTED)

Caso de uso

Enviado aos clientes cujos logs de SD-WAN mostraram **Indicadores de comprometimento (IoCs)** relacionados à consultoria PSIRT2a E que **reconstruíram anteriormente** sua malha. Fornece orientações atualizadas sobre correções com três opções (acompanhamento da Opção 2).

Assunto

Ação urgente necessária: Correção de vulnerabilidade crítica da infraestrutura SD-WAN - SR [SR#]

Mensagem

Caro cliente,

Obrigado por entrar em contato com o Cisco Technical Assistance Center (TAC) com relação aos avisos SD-WAN PSIRT recentes em Solicitação de serviço [SR#].

Depois de analisar os registros fornecidos pela malha da SD-WAN, nossa equipe identificou Indicadores de comprometimento (IOCs) associados à recomendação de vulnerabilidade da SD-WAN de 5 de junho de 2026. Também sabemos que seu ambiente passou anteriormente por uma reconstrução como parte das etapas de correção relacionadas a avisos anteriores.

Estamos fornecendo uma atualização importante para a correção da malha SD-WAN, conforme mencionado em [SR#] e nos avisos de segurança comunicados anteriormente. Esta atualização é específica para as malhas nas quais os registros fornecidos mostraram evidência de Indicadores de Comprometimento (IOCs).

Embora você tenha selecionado anteriormente um plano de reparo com base na Opção 2 — incorporando uma atualização de software, reimplantação de controlador e rotação de chaves SSH — nossa análise do cenário de ameaças continuou a evoluir. As novas informações técnicas sobre a exploração destas vulnerabilidades indicam que são fortemente exigidas medidas adicionais para reduzir o risco de persistência e ajudar a garantir a integridade da cadeia de certificados de confiança.

Ação exigida:

Atualizamos as estratégias de correção recomendadas para fornecer uma defesa mais abrangente, incluindo rotação adicional de certificados raiz.

Informamos que as correções exigirão atividades de manutenção adicionais, que podem incluir tempo de inatividade planejado da rede. Como nossa prioridade é a segurança e a integridade da sua rede, desenvolvemos três opções de correção distintas. Cada opção abaixo fornece um equilíbrio entre o impacto operacional e a garantia de segurança para sua consideração. Como sua postura interna de risco é única, a Cisco não pode recomendar um caminho específico.

Opção A: Reimplantação com reinicialização deslocável. Prioriza a continuidade operacional, evitando o tempo de inatividade da rede, embora apresente um risco residual de persistência de ameaças durante o processo de transição.

Descrição: Envolve a reimplantação do controlador, mais a chave SSH e a rotação de certificado. Os componentes do

controlador existentes são conectados durante a migração por meio do vManage para implantar a nova malha e, em seguida, cada um é removido assim que o dispositivo é migrado.

Opção B: Redistribuição com transição forçada. Fornece um nível mais alto de garantia de segurança. Como os novos controladores nunca se conectam a controladores antigos, há um isolamento completo. Devido a isso, há um impacto nas operações gerais da rede, pois todos os dispositivos precisam restabelecer a conectividade e trocar informações de rota/conectividade. O tempo de paralisação dependerá do número de locais, do número de prefixos trocados etc.

Descrição: Envolve a reimplantação do controlador mais a chave SSH e a rotação de certificado, mas os componentes antigos do controlador são isolados da nova malha durante a reimplantação.

Opção C: Reconstrução completa do sistema. Oferece o mais alto nível de garantia de segurança, estabelecendo uma linha de base limpa, embora seja a abordagem mais complexa e apresente um risco maior de instabilidade relacionada à configuração durante a reconstrução. Essa é uma opção demorada e exige experiência na reconstrução dos bancos de dados de modelos e políticas.

Assim que sua equipe tiver analisado essas opções e identificado a abordagem que melhor se alinha com seus padrões de gerenciamento de riscos, entre em contato conosco respondendo a esta mensagem. Ao recebermos sua seleção, coordenaremos a janela de manutenção e iniciaremos os preparativos técnicos necessários para a execução.

Agradecemos o seu foco contínuo na manutenção de uma infraestrutura de rede segura. Informe-nos se você precisar de mais esclarecimentos técnicos respondendo a este e-mail ou através da solicitação de serviço existente.

Atenciosamente,
Cisco

Abrir no Outlook

① Use o download .eml abaixo. Substitua todos os **[espaços reservados entre colchetes]** antes de enviar.

✉ Abrir Outlook (assunto apenas)

⬇ Baixar .eml Template

Modelo do TAC 11 para nenhum IOC para PSIRT2a/eles não reconstruíram (IMPACTADO ANTERIORMENTE)

Caso de uso

Enviado aos clientes cujos registros SD-WAN não mostraram **nenhum indicador de comprometimento (IoCs)** relacionado à consultoria PSIRT2a E que **NÃO reconstruíram** sua malha. Fornece orientações atualizadas sobre correções com três opções (acompanhamento da Opção 1).

Assunto

Ação urgente necessária: Correção de vulnerabilidade crítica da infraestrutura SD-WAN - SR [SR#]

Mensagem

Caro cliente,

Obrigado por entrar em contato com o Cisco Technical Assistance Center (TAC) com relação aos avisos SD-WAN PSIRT recentes em Solicitação de serviço [SR#].

Depois de analisar os registros e as informações fornecidas pela malha da SD-WAN, não identificamos os Indicadores de comprometimento (IOCs) associados ao aviso de vulnerabilidade da SD-WAN de 5 de junho de 2026.

Também sabemos que o ambiente não foi totalmente reconstruído de acordo com as recomendações anteriores. A Cisco recomenda revisar as diretrizes de remediação atualizadas abaixo para ajudar a reduzir a exposição potencial e fortalecer a integridade da cadeia de confiança do certificado de SD-WAN.

Com isso em mente, estamos fornecendo uma atualização crítica para a correção da sua estrutura SD-WAN, conforme referenciado em [SR#] e nos avisos de segurança comunicados anteriormente.

Embora você tenha selecionado anteriormente um plano de correção com base na Opção 1 — incorporando uma atualização de software e a rotação de chaves SSH — nossa análise do cenário de ameaças continuou a evoluir. As novas informações técnicas sobre a exploração destas vulnerabilidades indicam que são fortemente exigidas medidas adicionais para reduzir o risco de persistência e ajudar a garantir a integridade da cadeia de certificados de confiança.

Ação exigida:

Atualizamos as estratégias de correção recomendadas para fornecer uma defesa mais abrangente, incluindo rotação adicional de certificados raiz.

Informamos que as correções exigirão atividades de manutenção adicionais, que podem incluir tempo de inatividade planejado da rede. Como nossa prioridade é a segurança e a integridade da sua rede, desenvolvemos três opções de correção distintas. Cada opção abaixo fornece um equilíbrio entre o impacto operacional e a garantia de segurança para sua consideração. Como sua postura interna de risco é única, a Cisco não pode recomendar um caminho específico.

Opção A: Reimplantação com reinicialização deslocável. Prioriza a continuidade operacional, evitando o tempo de inatividade da rede, embora apresente um risco residual de persistência de ameaças durante o processo de transição.

Descrição: Envolve a reimplantação do controlador, mais a chave SSH e a rotação de certificado. Os componentes do controlador existentes são conectados durante a migração por meio do vManage para implantar a nova malha e, em seguida, cada um é removido assim que o dispositivo é migrado.

Opção B: Redistribuição com transição forçada. Fornece um nível mais alto de garantia de segurança. Como os novos controladores nunca se conectam a controladores antigos, há um isolamento completo. Devido a isso, há um

impacto nas operações gerais da rede, pois todos os dispositivos precisam restabelecer a conectividade e trocar informações de rota/conectividade. O tempo de paralisação dependerá do número de locais, do número de prefixos trocados etc.

Descrição: Envolve a reimplantação do controlador mais a chave SSH e a rotação de certificado, mas os componentes antigos do controlador são isolados da nova malha durante a reimplantação.

Opção C: Reconstrução completa do sistema. Oferece o mais alto nível de garantia de segurança, estabelecendo uma linha de base limpa, embora seja a abordagem mais complexa e apresente um risco maior de instabilidade relacionada à configuração durante a reconstrução. Essa é uma opção demorada e exige experiência na reconstrução dos bancos de dados de modelos e políticas.

Assim que sua equipe tiver analisado essas opções e identificado a abordagem que melhor se alinha com seus padrões de gerenciamento de riscos, entre em contato conosco respondendo a esta mensagem. Ao recebermos sua seleção, coordenaremos a janela de manutenção e iniciaremos os preparativos técnicos necessários para a execução.

Agradecemos o seu foco contínuo na manutenção de uma infraestrutura de rede segura. Informe-nos se você precisar de mais esclarecimentos técnicos respondendo a este e-mail ou através da solicitação de serviço existente.

Atenciosamente,
Cisco

Abrir no Outlook

① Use o download .eml abaixo. Substitua todos os *[espaços reservados entre colchetes]* antes de enviar.

✉ Abrir Outlook (assunto apenas)

↓ Baixar .eml Template

Modelo do TAC 12 para sim IOC para PSIRT2a/eles não reconstruíram (PREVIOUSLY IMPACTED)

Caso de uso

Enviado aos clientes cujos logs de SD-WAN mostraram **Indicadores de comprometimento (IoCs)** relacionados à consultoria PSIRT2a E que **NÃO reconstruíram** sua malha. Fornece orientações atualizadas sobre correções com três opções (acompanhamento da Opção 1).

Assunto

Ação urgente necessária: Correção de vulnerabilidade crítica da infraestrutura SD-WAN - SR [SR#]

Mensagem

Caro cliente,

Obrigado por entrar em contato com o Cisco Technical Assistance Center (TAC) com relação aos avisos SD-WAN PSIRT recentes em Solicitação de serviço [SR#].

Depois de analisar os registros fornecidos pela malha da SD-WAN, nossa equipe identificou Indicadores de comprometimento (IOCs) associados à recomendação de vulnerabilidade da SD-WAN de 5 de junho de 2026. Além disso, entendemos que seu ambiente não passou por uma reconstrução completa após as recomendações anteriores.

Dada a presença desses indicadores e a compreensão crescente do cenário de ameaças, é importante revisar e implementar as diretrizes de remediação atualizadas descritas abaixo para reduzir o risco de persistência e garantir a integridade da cadeia de confiança do certificado SD-WAN.

Estamos fornecendo uma atualização importante para a correção da malha SD-WAN, conforme mencionado em [SR#] e nos avisos de segurança comunicados anteriormente. Esta atualização é específica para as malhas nas quais os registros fornecidos mostraram evidência de Indicadores de Comprometimento (IOCs).

Embora você tenha selecionado anteriormente um plano de correção com base na Opção 1 — incorporando uma atualização de software e a rotação de chaves SSH — nossa análise do cenário de ameaças continuou a evoluir. As novas informações técnicas sobre a exploração destas vulnerabilidades indicam que são fortemente exigidas medidas adicionais para reduzir o risco de persistência e ajudar a garantir a integridade da cadeia de certificados de confiança.

Ação exigida:

Atualizamos as estratégias de correção recomendadas para fornecer uma defesa mais abrangente, incluindo rotação adicional de certificados raiz.

Informamos que as correções exigirão atividades de manutenção adicionais, que podem incluir tempo de inatividade planejado da rede. Como nossa prioridade é a segurança e a integridade da sua rede, desenvolvemos três opções de correção distintas. Cada opção abaixo fornece um equilíbrio entre o impacto operacional e a garantia de segurança para sua consideração. Como sua postura interna de risco é única, a Cisco não pode recomendar um caminho específico.

Opção A: Reimplantação com reinicialização deslocável. Prioriza a continuidade operacional, evitando o tempo de inatividade da rede, embora apresente um risco residual de persistência de ameaças durante o processo de transição.

Descrição: Envolve a reimplantação do controlador, mais a chave SSH e a rotação de certificado. Os componentes do controlador existentes são conectados durante a migração por meio do vManage para implantar a nova malha e, em seguida, cada um é removido assim que o dispositivo é migrado.

Opção B: Redistribuição com transição forçada. Fornece um nível mais alto de garantia de segurança. Como os novos controladores nunca se conectam a controladores antigos, há um isolamento completo. Devido a isso, há um impacto nas operações gerais da rede, pois todos os dispositivos precisam restabelecer a conectividade e trocar

informações de rota/conectividade. O tempo de paralisação dependerá do número de locais, do número de prefixos trocados etc.

Descrição: Envolve a reimplantação do controlador mais a chave SSH e a rotação de certificado, mas os componentes antigos do controlador são isolados da nova malha durante a reimplantação.

Opção C: Reconstrução completa do sistema. Oferece o mais alto nível de garantia de segurança, estabelecendo uma linha de base limpa, embora seja a abordagem mais complexa e apresente um risco maior de instabilidade relacionada à configuração durante a reconstrução. Essa é uma opção demorada e exige experiência na reconstrução dos bancos de dados de modelos e políticas.

Assim que sua equipe tiver analisado essas opções e identificado a abordagem que melhor se alinha com seus padrões de gerenciamento de riscos, entre em contato conosco respondendo a esta mensagem. Ao recebermos sua seleção, coordenaremos a janela de manutenção e iniciaremos os preparativos técnicos necessários para a execução.

Agradecemos o seu foco contínuo na manutenção de uma infraestrutura de rede segura. Informe-nos se você precisar de mais esclarecimentos técnicos respondendo a este e-mail ou através da solicitação de serviço existente.

Atenciosamente,
Cisco

Abrir no Outlook

① Use o download .eml abaixo. Substitua todos os **[espaços reservados entre colchetes]** antes de enviar.

✉ Abrir Outlook (assunto apenas)

↓ Baixar .eml Template

E-mails para WAVE 2A para NOVOS clientes (não afetados anteriormente)

Modelo do TAC 13 para IOC inexistente / Nenhuma versão fixa disponível (WAVE 2a — Aguarde a correção)

Caso de uso

Enviado a clientes cujos registros SD-WAN não mostraram **nenhum indicador de comprometimento (IoCs)** relacionado ao CVE-2026-20245, mas para os quais **nenhuma versão de software fixa está disponível no momento** para sua plataforma/versão. Aconselha o cliente a aplicar medidas provisórias de proteção e aguardar a notificação de liberação fixa.

Assunto

Atualizar: Avaliação da IoC concluída para CVE-2026-20245 - Nenhuma versão fixa disponível no momento - SR [SR#]

Mensagem

Caro cliente,

Obrigado por entrar em contato com o Cisco Technical Assistance Center (TAC) em relação ao CVE-2026-20245 sob Solicitação de serviço [SR#].

Concluimos a análise dos arquivos admin-tech fornecidos por você em seus componentes de controle da SD-WAN. **Não identificamos nenhum indicador de comprometimento (IoCs)** associado ao CVE-2026-20245 nos registros revisados.

Observe que a quantidade de dados de registro recuperados e fornecidos à Cisco para esta revisão pode ter sido limitada pelo período de retenção de registro configurado em seu ambiente de acordo com o [Guia de proteção de SD-WAN da Cisco](#)[1].

Importante — Não há versão de software fixa disponível no momento:

No momento, não há **nenhuma versão fixa de software disponível** para sua plataforma atual e versão de software para corrigir essa vulnerabilidade. A engenharia da Cisco está trabalhando ativamente para fornecer uma versão fixa. Quando o software fixo estiver disponível, o [aviso oficial de segurança](#)[2] será atualizado com as informações da versão fixa.

Ações intercalares recomendadas:

Enquanto aguarda a versão fixa, recomendamos enfaticamente a implementação das seguintes medidas de proteção para reduzir a sua exposição:

1. **Aplicar as práticas recomendadas de proteção:** Revise e implemente as recomendações do [Guia de proteção da Cisco SD-WAN](#)[1] para reduzir a superfície de ataque.
2. **Monitorar a Recomendação de Segurança:** Verifique periodicamente o [consultivo de segurança oficial](#)[2] para obter atualizações sobre a disponibilidade de versões fixas para sua plataforma.
3. **Plano de atualização:** Inicie o planejamento de atualização agora para que você esteja preparado para executar a atualização imediatamente após a publicação da versão fixa.
4. **Monitore seu ambiente:** Continue a monitorar seus componentes de controle da SD-WAN quanto a qualquer comportamento anômalo ou alterações inesperadas de configuração.

Próximas etapas:

Atualizaremos este caso quando a versão fixa do software estiver disponível. Nesse ponto, você deve priorizar a

atualização de todos os componentes de controle da SD-WAN (Gerenciador, Controlador, Validador) para a versão fixa assim que possível.

Se você tiver uma assinatura do BCS/LCS, entre em contato com seu Cisco NCE ou Gerente de entrega para obter orientação adicional sobre o planejamento de atualização.

Agradecemos sua paciência e seu compromisso com a segurança de sua infraestrutura. Se você tiver alguma dúvida ou precisar de mais assistência nesse ínterim, por favor, não hesite em responder a este caso.

Atenciosamente,
Cisco Technical Assistance Center (TAC)

Links:

[1] [Guia de proteção da Cisco SD-WAN](#)

[2] [Consultoria oficial de segurança \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

Abrir no Outlook

❗ Substitua todos os **[espaços reservados entre colchetes]** antes de enviar.

✉ Abrir Outlook (assunto apenas)

⬇ Baixar .eml Template

Modelo do TAC 14 para IOC/versão fixa não disponível (WAVE 2a — Atualize agora)

Caso de uso

Enviado aos clientes cujos registros SD-WAN não mostraram **nenhum indicador de comprometimento (IoCs)** relacionado ao CVE-2026-20245 E para os quais uma **versão fixa de software está disponível**. Aconselha o cliente a prosseguir com o planejamento e a execução da atualização imediatamente.

Assunto

Atualizar: Avaliação da IoC concluída para CVE-2026-20245 - Nenhum IoCs encontrado, atualização necessária - SR [SR#]

Mensagem

Caro cliente,

Obrigado por entrar em contato com o Cisco Technical Assistance Center (TAC) em relação ao CVE-2026-20245 sob Solicitação de serviço [SR#].

Concluímos a análise dos arquivos admin-tech fornecidos por você em seus componentes de controle da SD-WAN. **Não identificamos nenhum indicador de comprometimento (IoCs)** associado ao CVE-2026-20245 nos registros revisados.

Observe que a quantidade de dados de registro recuperados e fornecidos à Cisco para esta revisão pode ter sido limitada pelo período de retenção de registro configurado em seu ambiente de acordo com o [Guia de proteção de SD-WAN da Cisco](#)[1].

Importante — Atualização necessária:

Embora nenhum IoCs tenha sido identificado, a vulnerabilidade subjacente permanece presente até que seus componentes de controle da SD-WAN sejam atualizados para uma versão de software fixa. Uma versão fixa agora está disponível para sua plataforma.

Priorize **o planejamento e a execução da atualização** como a etapa mais importante na correção dessa vulnerabilidade. Se você ainda não agendou esta atualização, faça-o imediatamente.

Próximas etapas:

1. **Atualizar todos os componentes de controle da SD-WAN:** Atualize seu gerente (vManage), controlador (vSmart) e validador (vBond) para uma versão de software fixa listada no [consultivo de segurança oficial](#)[2].
2. **Recursos de atualização:** Consulte os seguintes documentos oficiais da Cisco para obter instruções detalhadas de atualização:
 - [Inicie a atualização do Catalyst SD-WAN](#)[3]
 - [Guia de atualização do Cisco SD-WAN](#)[4]
3. **Encerramento do caso:** Depois de concluir com êxito o upgrade de software em seu ambiente, você pode considerar esse caso resolvido e continuar com os procedimentos de fechamento padrão.

Se você tiver uma assinatura do BCS/LCS, entre em contato com seu Cisco NCE ou Gerente de entrega para obter orientação adicional sobre o processo de atualização.

Continuaremos monitorando seu caso. Se não recebermos resposta dentro de 10 dias úteis, presumiremos que não será necessária mais assistência e prosseguiremos com os procedimentos normais de encerramento de caso do TAC.

Atenciosamente,

Cisco Technical Assistance Center (TAC)

Links:

[1] [Guia de proteção da Cisco SD-WAN](#)

[2] [Consultoria oficial de segurança \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

[3] [Inicie a atualização do Catalyst SD-WAN](#)

[4] [Guia de atualização do Cisco SD-WAN](#)

Abrir no Outlook

① Substitua todos os *[espaços reservados entre colchetes]* antes de enviar.

✉ Abrir Outlook (assunto apenas)

⬇ Baixar .eml Template

Modelo do TAC 15 para IOC identificado/versão fixa disponível (WAVE 2a — Atualização urgente)

Caso de uso

Enviado aos clientes cujos registros SD-WAN mostraram **Indicadores de comprometimento (IoCs)** relacionados ao CVE-2026-20245 E para os quais uma **versão fixa de software está disponível**. Aconselha o cliente a atualizar com urgência e agendar uma chamada de revisão para discutir as descobertas e a correção.

Assunto

URGENTE: IoC identificada para CVE-2026-20245 - Atualização imediata necessária - SR [SR#]

Mensagem

Caro cliente,

Obrigado por entrar em contato com o Cisco Technical Assistance Center (TAC) em relação ao CVE-2026-20245 sob Solicitação de serviço [SR#].

Após analisar os arquivos de administração técnica fornecidos pelos componentes de controle da SD-WAN, nossa equipe **identificou os Indicadores de comprometimento (IoCs)** associados ao CVE-2026-20245.

Dada a natureza destas constatações, é fundamental que discutamos os pormenores técnicos e as próximas etapas recomendadas o mais rapidamente possível. Gostaríamos de agendar uma chamada com sua equipe para revisar as descobertas específicas e discutir o caminho de correção apropriado.

Ações imediatas necessárias:

- 1. Atualize imediatamente os componentes de controle da SD-WAN:** Uma versão de software fixa está disponível para sua plataforma. Atualize seu gerente (vManage), controlador (vSmart) e validador (vBond) para uma versão de software fixa listada no [consultivo de segurança oficial](#)^[1] assim que possível. A atualização fecha a vulnerabilidade imediatamente.
- 2. Agendar uma chamada de revisão:** Informe-nos sobre sua disponibilidade para uma breve chamada dentro das

próximas [por exemplo, 4-8 horas] para analisar as descobertas da IoC e discutir as opções de remediação recomendadas.

3. **Aplicar as práticas recomendadas de proteção:** Revise e implemente as recomendações do [Guia de proteção da Cisco SD-WAN](#)^[2] para reduzir a superfície de ataque enquanto a correção é planejada.

Recursos de atualização:

- [Inicie a atualização do Catalyst SD-WAN](#)^[3]
- [Guia de atualização do Cisco SD-WAN](#)^[4]

Importante: Após a atualização, etapas de correção adicionais (como reimplantação do controlador e rotação de certificado) podem ser recomendadas, dependendo da gravidade do comprometimento identificado. Eles serão discutidos durante a chamada de revisão.

Consulte também o [TAC Remediation Guide](#)^[5] para obter opções de correção detalhadas.

Nosso objetivo principal é ajudá-lo a proteger seu ambiente e mitigar quaisquer riscos potenciais. Agradecemos sua atenção imediata a este assunto e esperamos coordenar com você.

Atenciosamente,

Cisco Technical Assistance Center (TAC)

Links:

- [1] [Consultoria oficial de segurança \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)
- [2] [Guia de proteção da Cisco SD-WAN](#)
- [3] [Inicie a atualização do Catalyst SD-WAN](#)
- [4] [Guia de atualização do Cisco SD-WAN](#)
- [5] [Guia de correção do TAC](#)

Abrir no Outlook

① Substitua todos os *[espaços reservados entre colchetes]* antes de enviar.

✉ Abrir Outlook (assunto apenas)

⬇ Baixar .eml Template

Modelo do TAC 16 para IOC identificado / Nenhuma versão fixa disponível (WAVE 2a — Harden & Await Fix)

Caso de uso

Enviado aos clientes cujos registros SD-WAN mostraram **Indicadores de comprometimento (IoCs)** relacionados ao CVE-2026-20245, mas para os quais **não há nenhuma versão fixa de software disponível** para sua plataforma/versão. Aconselha o

fortalecimento imediato, agenda uma chamada de revisão e informa ao cliente que ele deve aguardar a versão fixa para corrigir totalmente o problema.

Assunto

URGENTE: IoC identificada para CVE-2026-20245 - Nenhuma versão fixa disponível atualmente - SR [SR#]

Mensagem

Caro cliente,

Obrigado por entrar em contato com o Cisco Technical Assistance Center (TAC) em relação ao CVE-2026-20245 sob Solicitação de serviço [SR#].

Após analisar os arquivos de administração técnica fornecidos pelos componentes de controle da SD-WAN, nossa equipe **identificou os Indicadores de comprometimento (IoCs)** associados ao CVE-2026-20245.

Dada a gravidade destas constatações, é fundamental que discutamos os pormenores técnicos e recomendemos medidas provisórias o mais rapidamente possível. Gostaríamos de agendar uma chamada com sua equipe para analisar as descobertas específicas.

Importante — Não há versão de software fixa disponível no momento:

No momento, não há **nenhuma versão fixa de software disponível** para a sua plataforma atual e versão de software para corrigir completamente essa vulnerabilidade. A engenharia da Cisco está trabalhando ativamente para fornecer uma versão fixa. Quando o software fixo estiver disponível, o [aviso de segurança oficial](#)[1] será atualizado com as informações da versão fixa.

Ações imediatas necessárias:

1. **Agendar uma chamada de revisão:** Informe-nos sobre sua disponibilidade para uma breve chamada dentro das próximas [por exemplo, 4 a 8 horas] para analisar os resultados da IoC e discutir medidas provisórias de contenção.
2. **Aplique as práticas recomendadas de proteção imediatamente:** Revise e implemente as recomendações do [Guia de proteção da Cisco SD-WAN](#)[2] para reduzir a superfície de ataque enquanto aguarda a liberação fixa.
3. **Monitoramento aprimorado:** Monitore atentamente seus componentes de controle da SD-WAN quanto a qualquer comportamento anômalo, alterações inesperadas de configuração ou tentativas de acesso não autorizado.
4. **Monitorar a Recomendação de Segurança:** Verifique periodicamente o [consultivo de segurança oficial](#)[1] para obter atualizações sobre a disponibilidade de versões fixas para sua plataforma.
5. **Plano de atualização:** Inicie o planejamento de atualização agora para que você esteja preparado para executar a atualização imediatamente após a publicação da versão fixa.

Próximas etapas:

Atualizaremos este caso quando a versão fixa do software estiver disponível. Nesse ponto, você deve priorizar a atualização de todos os componentes de controle da SD-WAN (Gerenciador, Controlador, Validador) para a versão fixa imediatamente. Após a atualização, etapas de correção adicionais (como reimplantação do controlador e rotação de certificado) serão discutidas com base nas descobertas analisadas durante nossa chamada.

Consulte também o [TAC Remediation Guide](#)[3] para obter informações sobre as opções de correção que serão aplicadas quando a versão fixa estiver disponível.

Nosso objetivo principal é ajudá-lo a proteger seu ambiente e mitigar quaisquer riscos potenciais. Agradecemos sua atenção imediata a este assunto e esperamos coordenar com você.

Atenciosamente,

Cisco Technical Assistance Center (TAC)

Links:

[1] [Consultoria oficial de segurança \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

[2] [Guia de proteção da Cisco SD-WAN](#)

[3] [Guia de correção do TAC](#)

Abrir no Outlook

① Substitua todos os **[espaços reservados entre colchetes]** antes de enviar.

✉ Abrir Outlook (assunto apenas)

⬇ Baixar .eml Template

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.