

检查已有文章的粗体

目录

[简介](#)

[参考 — Cisco SD-WAN CVE-2026-20182文档](#)

[电子邮件](#)

[Sherlock 1 — 录入 — 请求升级和管理技术文件](#)

[Sherlock 2 — 结果 — 未观察到任何IoC \(每个文件\)](#)

[Sherlock 3 — 提醒 — 丢失管理技术文件](#)

[TAC 1 — 调查 — 需要进一步审查 \(疑似IoC\)](#)

[TAC 2 — 结果 — 未找到IoC \(工程师确认\)](#)

[TAC 3 — 验证 — 确认重叠中的IP所有权](#)

[TAC 4 — 结果 — 已清除误报](#)

[TAC 5 — 重要 — 确定IoC, 安排审核呼叫](#)

[TAC 6 — 结果 — 重复的IoC \(关闭和重定向\)](#)

[TAC 7 — 补救 — 选项跟进 \(呼叫后\)](#)

[TAC 8 — 补救 — 受危害交换矩阵的更新选项 \(选项2后续步骤\)](#)

[TAC 17 — 反向发现 — 以前没有IoC, 现在已识别IoC\(CVE-2026-20182\)](#)

[CloudOps 1 — 主动 — 在云扫描中检测到IoC, 需要管理员技术以进行验证](#)

[针对尚未完成选项A、B或C的以前受影响的客户的WAVE 2A电子邮件。\(选项1和2需要重新完成\)](#)

[TAC 9模板, 无适用于PSIRT2a的IOC/它们确实重建 \(以前受影响\)](#)

[TAC 10模板, 表示是IOC for PSIRT2a/它们确实重建 \(以前受影响\)](#)

[TAC 11模板, 无适用于PSIRT2a的IOC/它们未重建 \(之前受影响\)](#)

[TAC 12 Template for yes IOC for PSIRT2a/they not rebuild\(PREVIOUSLY IMPACTED\)](#)

[新客户的WAVE 2A电邮 \(之前未受影响\)](#)

[TAC 13模板, 无IOC/无可用的固定版本 \(WAVE 2a — 等待修复\)](#)

[TAC 14模板, 无可用的IOC/固定版本 \(WAVE 2a — 立即升级\)](#)

[TAC 15模板, 用于确定IOC/提供固定版本 \(WAVE 2a — 紧急升级\)](#)

[确定IOC的TAC 16模板/无可用的固定版本 \(WAVE 2a — 强化并等待修复\)](#)

简介

本文档集中了与Cisco Catalyst SD-WAN控制器身份验证绕行漏洞相关的案例的分类和补救过程中使用的已批准客户邮件模板。模板按发件人 — Sherlock (收集管理员技术数据并返回初步IoC结果的自动案例交换) 和TAC工程师 (调查、验证和补救指导的人工驱动后续操作) 进行拆分。

参考 — Cisco SD-WAN CVE-2026-20182文档

以上电邮模板中引用的每个思科文档的主列表。统一编号 — 每个邮件上标(例如^[2])指向此列表中的项目。

1. 思科SD-WAN加固指南— <https://sec.cloudapps.cisco.com/security/center/resources/Cisco-Catalyst-SD-WAN-HardeningGuide>
2. 官方安全公告(cisco-sa-sdwan-mltnps2-JxpWm7R)—
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>
3. TAC修复指南 — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225842-remediate-catalyst-sd-wan-security.html#toc-hld--1516256622>
4. Cisco SD-WAN升级指南— <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>
5. 思科SD-WAN管理技术收集指南— <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. 第二个安全建议(cisco-sa-sdwan-rpa2-v69WY2SW)—
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>
7. 开始Catalyst SD-WAN升级— <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

电子邮件

Sherlock 1 — 录入 — 请求升级和管理技术文件

使用案例

为CVE-2026-20182打开TAC支持请求时，建议从收集管理技术数据，然后升级所有SD-WAN控制组件，从而进行初始推广。

主题

重要信息： CVE-2026-20182 — 升级规划和IoC评估所需操作

邮件

亲爱的用户：

感谢您联系思科技术支持中心(TAC)。

有关CVE-2026-20182相关的漏洞，请查看[官方安全建议](#)^[1]，了解完整详情以及[TAC补救指南](#)^[2]。

我们的主要目标是帮助保护您的环境。请**优先安排升级规划和执行**，作为降低此风险的最重要步骤。如果您尚未安排此升级，请立即执行此操作。

升级资源：有关如何执行升级的详细说明，请参阅以下思科官方文档：[思科SD-WAN升级指南](#)^[3]

要针对与CVE-2026-20182相关的任何潜在危害表现(loC)对您的环境进行初始评估，必须在升级之前执行管理 — 技术收集(admin-tech collection)。请遵循以下操作顺序：

1. **收集管理技术文件**：在升级之前，从所有SD-WAN控制组件生成管理技术日志，以确保不会丢失诊断数据。生成这些文件时，请确保您选择“日志”和“技术”。
 - **vSmarts (控制器)**：一次收集一个，而不是同时收集。
 - **vBonds (验证程序)**：从所有节点收集。
 - **管理器(vManage)**:从集群中的所有节点 (活动和备用DR) 收集。
2. **执行升级**：将所有SD-WAN控制组件(vManage、vSmart、vBond)升级到顾问中列出的固定软件版本。不要等待管理技术日志分析后再开始升级，因为升级会立即关闭漏洞。
3. **上传到TAC案例**：升级完成后，如有可能，将之前收集的文件同时上传到现有的TAC案例。然后，我们的团队将对这些日志进行扫描，以评估您的环境中是否存在危害表现(loC)。

资源和支持：

有关生成和安全提交管理技术文件的更多详情和分步说明，请参阅本指南：[思科SD-WAN管理技术收集指南](#)^[4]。

如果您有BCS/LCS订用，请联系Cisco NCE或Delivery Manager获取有关升级过程或后续步骤的其他指导。

您的数据隐私和安全仍然是我们的首要任务。提供的所有信息都将根据思科的隐私和安全策略进行处理。

对于成功上传到案例的每个文件，您将收到自动电子邮件确认；请确保您查看这些通知。

感谢您在保护基础设施方面迅速合作。

链接：

[1]官方[安全建议](#)

[2] TAC[补救指南](#)

[3]思科[SD-WAN升级指南](#)

[4] [Cisco SD-WAN管理技术收集指南](#)

顺致敬意！

在Outlook中打开

①使用下面的.eml下载。在发送之前，替换所有[括号中的占位符]。

✉ 打开Outlook（仅主题）

📎 下载.eml模板

Sherlock 2 — 结果 — 未观察到任何IoC（每个文件）

使用案例

在管理技术分析后发送：对于特定上传的文件，没有观察到危害表现。每个处理的文件发送一次。

主题

更新：SD-WAN组件[插入文件名] - CVE-2026-20182的分析结果

邮件

亲爱的用户：

感谢您的耐心。

我们已完成对admin-tech文件[插入文件名]的分析。在该文件中，我们没有识别出与此特定设备的CVE-2026-20182相关的任何危害表现。

请注意，您检索并提供给思科用于本次审查的日志数据量可能受到您根据Cisco SD-WAN强化指南^[1]配置的日志保留期的限制。

重要信息：后续步骤和案例关闭：

1. **等待所有结果：**请注意，此电子邮件中的结果可能是部分结果。我们将分析提供的每个文件。请等到收到所有上传文件的确认后再考虑考试完成。
2. **升级优先级：**虽然管理技术日志的初步扫描尚未识别危害表现(IoC)，但底层漏洞可能仍然存在。对于Cisco Cloud-Pro和Cisco On-Prem部署，如果您尚未执行此操作，请尽快确定您的SD-WAN控制组件全面升级的优先顺序。
 - 思科云(fka:SaaS)客户交换矩阵由思科自动升级，作为托管服务的一部分。 无需任何操作。

3. 案例结束：当您收到所有上传文件的“未观察IoC”结果并且（如果适用）您已成功完成整个环境的软件升级后，您可以考虑解决此问题并继续执行标准关闭过程。

升级资源（如果适用）：有关如何执行思科云专业版和思科内部版升级的详细说明，请参阅以下思科官方文档：Cisco SD-WAN升级指南

升级过程的高级概述包括：

1. 将相应的软件映像上传到Manager(vManage)存储库。
2. 按顺序升级控制器，从管理器(vManage)开始，接着是验证器(vBond)和控制器(vSmart)。
3. 激活新软件版本并验证系统功能。

我们将继续监视您的案例。如果我们根据从您那里收到的文件提供所有结果后，在10个工作日内没有收到回复，我们假定无需进一步帮助，并继续进行正常的TAC案例解决程序。如果您需要帮助，请告诉我们。

顺致敬意！

在Outlook中打开

① 发送前替换所有[带括号的占位符]。

✉ 打开Outlook（仅主题）

↓ 下载.eml模板

Sherlock 3 — 提醒 — 丢失管理技术文件

使用案例

提交的管理技术文件与日志中找到的SD-WAN控制组件数量不匹配时自动跟进。

主题

提醒：CVE-2026-X评估所需的管理技术文20182丢失

邮件

亲爱的用户：

SD-WAN控制组件中仍然缺少管理技术，因此我们的系统无法通过管理技术日志评估任何危害表现。

要开始CVE-2026-20182评估，我们必须接收来自所有控制器(vSmarts)、验证器(vBonds)和管理器(vManage)的管理技术文件，包括集群中的所有管理器(vManage)节点。

后续方案

请尽快上传剩余的管理技术文件。

顺致敬意！

在Outlook中打开

① 发送前替换所有[带括号的占位符]。

✉ 打开Outlook（带正文）

↓ 下载.eml模板

TAC 1 — 调查 — 需要进一步审查（疑似IoC）

使用案例

自动化发现可能危害的日志后，TAC工程师发送此消息，需要进行人工调查。

主题

SR编号 — 需要进一步调查

邮件

亲爱的用户：

我的名字是{your_name}，我接受了您的案例。感谢您继续与思科技术支持中心(TAC)合作。

在对您从SD-WAN控制组件提供的管理技术文件进行初步分析后，我们确定需要进行TAC进一步调查才能完成我们的分析。为了帮助确保彻底而准确地解决问题，我将与您密切合作，执行后续步骤。

请放心，我们将致力于支持您完成这些后续步骤，并将提供明确指导，帮助您有效应对这种情况。

请确定升级规划和执行的优先顺序，将其作为降低此风险的最关键步骤。如果您尚未安排此升级，请立即执行此操作。

如果您有任何疑问或需要帮助，请随时联系您的TAC工程师。

感谢您的关注和协作。

顺致敬意！

在Outlook中打开

① 发送前替换所有[带括号的占位符]。

✉ 打开Outlook（带正文）

↓ 下载.eml模板

TAC 2 — 结果 — 未找到IoC（工程师确认）

使用案例

在自动化未发现任何危害表现，且工程师已确认结果后，由TAC工程师发送。

主题

更新：TAC审核完成 — 未找到CVE-2026-20182的IoC — 案例[SR #]

邮件

[客户姓名]，您好！

我是分配给您的案例[SR Number]的思科TAC工程师。

对您从SD-WAN控制组件提供的管理技术文件执行初步扫描后，我们找不到与思科SD-WAN安全建议中描述的危害表现相符的日志条目：

- Cisco Catalyst SD-WAN控制器身份验证旁路漏洞[1]
- Cisco Catalyst SD-WAN Manager漏洞[2]

但是，您应该继续将所有SD-WAN控制组件升级到<insert version>。 以下是继续升级的步骤：

- 开始Catalyst SD-WAN升级[3]
- 思科SD-WAN升级指南[4]

请注意，由于互联网IP编址的动态性质以及我们对客户网络中边缘设备的预期IP地址缺乏了解，思科无法评估边缘设备的日志。鼓励客户遵循Cisco Catalyst SD-WAN控制器身份验证旁路漏洞安全建议中所述的对等事件验证指南手动完成此步骤。此外，还鼓励客户完成与CVE-2026-20182安全建议中所述的对等事件验证相关的其他检测步骤。

链接

[1] Cisco Catalyst SD-WAN控制器身份验证旁路漏洞 —

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

[2] Cisco Catalyst SD-WAN Manager漏洞 —

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

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

[4]思科SD-WAN升级指南 — <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>

顺颂商祺

在Outlook中打开

① 发送前替换所有[带括号的占位符]。

✉ 打开Outlook (仅主题)

📎 下载.eml模板

TAC 3 — 验证 — 确认重叠中的IP所有权

使用案例

由TAC工程师发送，询问客户在日志分析期间出现的特定IP地址是属于还是属于其SD-WAN重叠基础设施的一部分。

主题

[SR #] — 需要IP地址验证

邮件

尊敬的[客户名称]:

我是[您的姓名]，是您的案例的Cisco TAC工程师。

作为我们持续分析您从SD-WAN控制组件提供的管理技术文件的一部分，我们需要您帮助验证以下IP地址是否属于或曾经属于您的SD-WAN重叠基础设施：

有问题的IP地址：

- [IP地址1]

- [IP地址2]

为了帮助我们完成评估，请确认：

- 1.此IP地址当前是否与SD-WAN重叠中的任何组件相关联（例如，vManage、vSmart、vBond或边缘设备）？
- 2.此IP地址以前是否曾被任何可能已停用或其IP已更改的SD-WAN控制组件使用？
- 3.此IP是否与灾难恢复(DR)站点或与您的SD-WAN部署相关的任何其他基础设施相关联？

您的迅速反应将让我们继续进行分析，并向您提供相应的后续步骤。

如有任何疑问，请随时联系。

顺致敬意！

在Outlook中打开

① 发送前替换所有[方括号中的占位符]。

✉ 打开Outlook（带正文）

↓ 下载.eml模板

TAC 4 — 结果 — 已清除误报

使用案例

在手动审核确定自动扫描所标记的初始IoC为误报后，由TAC工程师发送。

主题

更新：CVE-2026-20182技术审查 — 案例[案例编号]

邮件

亲爱的用户：

感谢您耐心等待，我们的工程团队手动审核您从SD-WAN控制组件提供的管理技术文件。

通过彻底的调查，我们确定我们的自动扫描流程所标记的初始危害表现(loC)是误报，即我们的评估是loC无效。

重要信息：虽然此特定警报已被清除，但请注意，与[CVE-2026-20182](#)^[1]相关的漏洞需要进行软件升级，以帮助确保SD-WAN交换矩阵的长期安全性和完整性。

如果您尚未完成升级：请尽快确定您的SD-WAN控制组件全面升级的优先顺序。升级是有效修复此漏洞的唯一方法。有关详细说明，请参阅[Cisco SD-WAN升级指南](#)^[2]。

如果您已完成升级：由于我们已将此调查结果确认为误报，并且您已执行了软件补救，因此无需执行进一步操作。您可以认为此问题已解决并继续执行标准关闭过程。

我们非常感谢您对基础设施安全给予优先考虑。如有任何进一步问题或需要额外帮助，请随时联系我们。

顺致敬意！

Cisco 技术支持中心 (TAC)

链接：

[1]官方[安全建议](#)

[2] [Cisco SD-WAN升级指南](#)

在Outlook中打开

① 发送前替换所有[带括号的占位符]。

✉ 打开Outlook (仅主题)

📎 下载.eml模板

TAC 5 — 重要 — 确定loC，安排审核呼叫

使用案例

TAC工程师在确认潜在危害表现时发送此消息，并需要紧急客户电话来讨论调查结果和后续步骤。

主题

紧急:CVE-2026-20182的分析结果 — 确定危害指标

邮件

亲爱的用户：

感谢您耐心等待我们分析为SD-WAN控制组件提供的管理技术文件。

通过技术审查，我们确定了与CVE-2026-20182相关的潜在危害表现(LoC)。

鉴于这些调查结果的性质，我们必须尽快讨论技术细节和建议的后续步骤。我们希望与您的团队安排一次电话会议，以审查具体的调查结果并讨论适当的补救措施。

后续方案

- **安排会议:**请在接下来的[例如4-8小时]内向我们提供简短电话来审阅这些调查结果。
- **升级SDWAN控制组件:**请尽快将您的SDWAN Manager、Controller和Validator升级到固定版本。

我们的主要目标是帮助您保护环境和降低任何潜在风险。我们感谢您迅速关注此事，并期待与您协调。

顺致敬意！

在Outlook中打开

① 发送前替换所有[带括号的占位符]。

✉ 打开Outlook (带正文)

📎 下载.eml模板

TAC 6 — 结果 — 重复的LoC (关闭和重定向)

使用案例

当LoC分析确认与同一客户/环境的早期SR相匹配的结果时，由TAC工程师发送。当前案例已关闭，客户将被重定向至已提供补救指导的原始SR。

主题

更新：CVE-2026-20182技术审查 — 案例[SR #] (确认重复LoC)

邮件

亲爱的用户：

感谢您耐心等待我们分析为SD-WAN控制组件提供的管理技术文件。我们确定，扫描流程所标记的初始危害表现(loC)与[原始SR编号]中已经传达的指标相同。如前所述，我们建议紧急升级，然后按照[TAC补救指南](#)^[2]中概述的两种补救路径之一进行更新，以尽快保护您的环境。有关完整详情，请参阅[CVE-2026-20182](#)^[1]的官方安全公告。

我现在将结束此案例。请使用[原始SR编号]请求有关升级或补救的进一步指导或技术支持。

顺致敬意！

[您的名字]

链接：

[1]官方[安全建议](#)

[2] TAC[补救指南](#)

在Outlook中打开

① 发送前替换所有[带括号的占位符]。

✉ 打开Outlook（带正文）

📄 下载.eml模板

TAC 7 — 补救 — 选项跟进（呼叫后）

使用案例

在loC审核呼叫后发送，以总结所讨论的补救路径。客户选择选项A（通过滚动重启重新部署）、选项B（通过硬切换重新部署）或选项C（完整系统重建）。

主题

后续步骤：CVE-2026-20182的补救选项

邮件

亲爱的用户：

感谢您抽出宝贵时间讨论我们最近的分析结果。正如我们在前一次通话中讨论的那样，我们建议使用以下补救路径之一来保护您的环境。

方案 A：通过滚动重启重新部署。通过避免网络停机来优先处理运营连续性，尽管它在过渡过程中仍存在威胁持久性的风险。

描述:涉及控制器重新部署，以及SSH密钥和证书轮换。在迁移期间，通过vManage连接现有控制器组件以部署新交换矩阵，并在设备迁移后立即删除每个控制器组件。

方案 B：通过硬切换重新部署。提供更高级别的安全保证。由于新控制器从未连接到旧控制器，因此存在完全隔离。由于所有设备都需要重新建立连接并交换路由/连接信息，因此这会对整体网络运营造成影响。中断时间将取决于站点数量、交换的前缀数量等。

描述:涉及控制器重新部署以及SSH密钥和证书轮换，但在重新部署期间，旧控制器组件与新交换矩阵隔离。

方案C:完全重建系统。通过建立干净的基线提供最高级别的安全保证，尽管这是最复杂的方法，并且在重建期间存在与配置相关的不稳定风险。这是一个漫长的选项，需要具备重建模板和策略数据库的专业知识。

后续方案

- 请在内部讨论这些选项，并告诉我们您打算采用哪条路径。一旦您做出决定，我们可提供进一步指导或技术支持，帮助您完成执行阶段。

我们在此支持您完成整个流程。如果您对这些选项有任何疑问，请告诉我们。

顺致敬意！

Cisco 技术支持中心 (TAC)

NOTE:选项1是升级。认为此升级已执行的场景。

在Outlook中打开

①使用下面的 .eml 下载。在发送之前，替换所有[括号中的占位符]。

✉ 打开 Outlook (仅主题)

↓ 下载 .eml 模板

TAC 8 — 补救 — 受危害交换矩阵的更新选项 (选项2后续步骤)

使用案例

通知其SD-WAN交换矩阵遭到入侵且以前追求的选项2，以及认为其交换矩阵存在威胁实施者持久性风险的客户。重建受损交换矩阵 (并且不依赖于备份/现有configDB) 的客户不会被视作有风险，也不会收到此通信。此通信将由TBD发送。

主题

需要采取紧急行动：SD-WAN基础设施关键漏洞补救

邮件

亲爱的用户：

我们提供关键更新来补救您的SD-WAN交换矩阵，如[SR#]和之前传达的安全公告中所述。此更新特定于所提供日志显示危害表现(IOC)证据的交换矩阵。

虽然您之前选择了基于选项2（包括软件升级、控制器重新部署和SSH密钥轮换）的补救计划，但是我们对威胁形势的分析仍在继续发展。关于利用这些漏洞的新技术见解表明，强烈敦促采取其他措施，以降低持续存在的风险，并帮助确保证书信任链的完整性。

需执行的操作：

我们更新了推荐的补救策略，通过包含额外的根证书轮换来提供更全面的防御。

请注意，补救措施需要执行额外的维护活动，其中可能包括计划内网络停机时间。

鉴于我们的首要任务是确保网络的安全性和完整性，我们制定了三种不同的补救方案。以下每个选项均提供运营影响与安全保证之间的平衡，供您考虑。由于您的内部风险状况是唯一的，思科无法推荐特定路径。

方案 A：通过滚动重启重新部署。通过避免网络停机来优先处理运营连续性，尽管它在过渡过程中仍存在威胁持久性的风险。

描述：涉及控制器重新部署，以及SSH密钥和证书轮换。在迁移期间，通过vManage连接现有控制器组件以部署新交换矩阵，并在设备迁移后立即删除每个控制器组件。

方案 B：通过硬切换重新部署。提供更高级别的安全保证。由于新控制器从未连接到旧控制器，因此存在完全隔离。由于所有设备都需要重新建立连接并交换路由/连接信息，因此这会对整体网络运营造成影响。中断时间将取决于站点数量、交换的前缀数量等。

描述：涉及控制器重新部署以及SSH密钥和证书轮换，但在重新部署期间，旧控制器组件与新交换矩阵隔离。

方案C：完全重建系统。通过建立干净的基线提供最高级别的安全保证，尽管这是最复杂的方法，并且在重建期间存在与配置相关的不稳定风险。这是一个漫长的选项，需要具备重建模板和策略数据库的专业知识。

在您的团队审查了这些选项并确定了与您的风险管理标准最相符的方法后，请回复此邮件通知我们。收到您的选择后，我们将协调维护窗口，开始必要的技术准备以执行。

感谢您一如既往地专注于维护安全的网络基础设施。如果您需要在我们的技术支持中心(TAC)提交服务请求(SR)，以便进一步进行技术说明，请通知我们。

此致，
思科

在Outlook中打开

①使用下面的 .eml 下载。在发送之前，替换所有[括号中的占位符]。

✉ 打开 Outlook (仅主题)

📎 下载 .eml 模板

TAC 17 — 反向发现 — 以前没有IoC，现在已识别IoC(CVE-2026-20182)

使用案例

发送给之前通知未发现危害表现符(IoC)的客户，但随后对管理技术日志的内部审核已识别出与CVE-2026-20182相关的IoC的客户。传达修改后的发现结果并提供三个补救选项（选项A、B或C）。

主题

重要更新：CVE-2026-20182的修订版IoC评估 — 现已确定危害表现 — SR [SR#]

邮件

亲爱的用户：

感谢您继续与思科技术支持中心(TAC)就服务请求[SR#]项下的CVE-2026-20182开展合作。

在之前的通信中，我们建议对从您的SD-WAN控制组件提供的管理技术文件的分析没有识别与此建议相关的任何危害表现(IoC)。作为对您安全保护持续承诺的一部分，我们随后对与您组织的交换矩阵相关的其他管理技术日志数据进行了例行内部审核。

此后的审查确定了初次评估期间未出现的危害表现(IoC)。我们现在正与您合作解决这些发现问题。这些IoC指示组织交换矩阵中可能的可疑活动，从而需要采取补救措施。

我们认识到这会修改先前传达给您的结果，并且我们希望确保您清楚准确地了解您的环境，以便采取适当的补救措施。

需执行的操作：

请注意，补救措施需要执行额外的维护活动，其中可能包括计划内网络停机时间。

鉴于我们的首要任务是确保网络的安全性和完整性，我们制定了三种不同的补救方案。以下每个选项

均提供运营影响与安全保证之间的平衡，供您考虑。由于您的内部风险状况是唯一的，思科无法推荐特定路径。

方案 A：通过滚动重启重新部署。通过避免网络停机来优先处理运营连续性，尽管它在过渡过程中仍存在威胁持久性的风险。

描述:涉及控制器重新部署，以及SSH密钥和证书轮换。在迁移期间，通过vManage连接现有控制器组件以部署新交换矩阵，并在设备迁移后立即删除每个控制器组件。

方案 B：通过硬切换重新部署。提供更高级别的安全保证。由于新控制器从未连接到旧控制器，因此存在完全隔离。由于所有设备都需要重新建立连接并交换路由/连接信息，因此这会对整体网络运营造成影响。中断时间将取决于站点数量、交换的前缀数量等。

描述:涉及控制器重新部署以及SSH密钥和证书轮换，但在重新部署期间，旧控制器组件与新交换矩阵隔离。

方案C:完全重建系统。通过建立干净的基线提供最高级别的安全保证，尽管这是最复杂的方法，并且在重建期间存在与配置相关的不稳定风险。这是一个漫长的选择，需要重建模板和策略数据库的专业知识。

在您的团队审查了这些选项并确定了与您的风险管理标准最相符的方法后，请回复此邮件通知我们。收到您的选择后，我们将协调维护窗口，开始必要的技术准备以执行。

感谢您一如既往地专注于维护安全的网络基础设施。如果您希望通过回复本电子邮件或通过我们的技术支持中心(TAC)的现有服务请求(SR)进一步了解技术信息，请告诉我们。

此致，
思科

在Outlook中打开

①使用下面的 .eml 下载。在发送之前，替换所有[括号中的占位符]。

✉ 打开 Outlook (仅主题)

📎 下载 .eml 模板

CloudOps 1 — 主动 — 在云扫描中检测到IoC，需要管理员技术以进行验证

使用案例

当云托管SD-WAN交换矩阵的Cisco CloudOps安全扫描出现潜在危害表现(IoC)时主动发送。代表客户打开一个SR，要求客户附加管理技术文件，以便通过完整的日志分析来验证调查结果。

主题

需采取的行动：验证安全扫描结果所需的管理技术文件 — SR [SR#]

邮件

亲爱的用户：

作为我们对保护和监控思科产品完整性的持续承诺的一部分，思科最近完成了选定云托管SD-WAN交换矩阵的安全扫描。这一行动是应所报告的安全关切采取的。扫描已识别组织交换矩阵中可能的可疑活动，需要进一步检查。

我们请求您的帮助，以将管理员技术文件附加到以您的名义打开的此服务请求(SR)，以便我们可以验证此发现并完成调查。

要启用完整分析，请收集并上传所有SD-WAN控制组件中的管理技术文件。在生成以下文件时，确保选择“日志”和“技术”：

- **vSmarts (控制器)**：一次收集一个，而不是同时收集。
- **vBonds (验证程序)**：从所有节点收集。
- **管理器(vManage)**：从集群中的所有节点（活动和备用DR）收集。

有关生成和安全提交管理技术文件的详细分步说明，请参阅本指南：[思科SD-WAN管理技术收集指南](#)^南
[1]。

收到请求的文件后，我们的团队将对其进行分析以确认观察到的活动是否代表真正的危害表现，并将就适当的后续步骤向您提出建议。

感谢您一如既往地专注于维护安全的网络基础设施。如果您在回复本服务请求(SR)时需要进一步的技术说明，请告知我们。

顺致敬意！

思科

链接：

[1] [Cisco SD-WAN管理技术收集指南](#)

在Outlook中打开

①使用下面的 .eml 下载。在发送之前，替换所有[括号中的占位符]。

✉ 打开Outlook（仅主题）

↓ 下载.eml模板

针对尚未完成选项A、B或C的以前受影响的客户的WAVE 2A电子邮件。（选项1和2需要重新完成）

TAC 9模板，无适用于PSIRT2a的IOC/它们确实重建(之前受影响)

使用案例

发送给其SD-WAN日志未显示与PSIRT2a建议相关的危害表现(IoC)以及之前重建交换矩阵的客户的邮件。提供更新的补救指南，提供三个选项（选项2后续选项）。

主题

需要采取紧急行动：SD-WAN基础设施关键漏洞补救 — SR [SR#]

邮件

亲爱的用户：

感谢您联系思科技术支持中心(TAC)，了解服务请求[SR#]下最近的SD-WAN PSIRT建议。

在检查了从您的SD-WAN交换矩阵提供的日志和信息后，我们的分析未发现与2026年6月5日SD-WAN漏洞通知相关的任何危害表现(IoC)。此外，我们了解您的环境之前已进行了重建，这是与早期建议相关的补救措施的一部分。

考虑到与这些漏洞相关的新发现的见解，我们想要分享有关建议的SD-WAN交换矩阵补救指南的重要更新。

我们提供关键更新来补救您的SD-WAN交换矩阵，如[SR#]和之前传达的安全公告中所述。

虽然您之前选择了基于选项2（包括软件升级、控制器重新部署和SSH密钥轮换）的补救计划，但是我们对威胁形势的分析仍在继续发展。关于利用这些漏洞的新技术见解表明，强烈敦促采取其他措施，以降低持续存在的风险，并帮助确保证书信任链的完整性。

需执行的操作：

我们更新了推荐的补救策略，通过包含额外的根证书轮换来提供更全面的防御。

请注意，补救措施需要执行额外的维护活动，其中可能包括计划内网络停机时间。鉴于我们的首要任务是确保网络的安全性和完整性，我们制定了三种不同的补救方案。以下每个选项均提供运营影响与安全保证之间的平衡，供您考虑。由于您的内部风险状况是唯一的，思科无法推荐特定路径。

方案 A：通过滚动重启重新部署。通过避免网络停机来优先处理运营连续性，尽管它在过渡过程中仍

存在威胁持久性的风险。

描述:涉及控制器重新部署，以及SSH密钥和证书轮换。在迁移期间，通过vManage连接现有控制器组件以部署新交换矩阵，并在设备迁移后立即删除每个控制器组件。

方案 B：通过硬切换重新部署。提供更高级别的安全保证。由于新控制器从未连接到旧控制器，因此存在完全隔离。由于所有设备都需要重新建立连接并交换路由/连接信息，因此这会对整体网络运营造成影响。中断时间将取决于站点数量、交换的前缀数量等。

描述:涉及控制器重新部署以及SSH密钥和证书轮换，但在重新部署期间，旧控制器组件与新交换矩阵隔离。

方案C:完全重建系统。通过建立干净的基线提供最高级别的安全保证，尽管这是最复杂的方法，并且在重建期间存在与配置相关的不稳定风险。这是一个漫长的选择，需要重建模板和策略数据库的专业知识。

在您的团队审查了这些选项并确定了与您的风险管理标准最相符的方法后，请回复此邮件通知我们。收到您的选择后，我们将协调维护窗口，开始必要的技术准备以执行。

感谢您一如既往地专注于维护安全的网络基础设施。如果您需要通过回复此电子邮件或通过现有的服务请求进一步进行技术说明，请告知我们。

此致，
思科

在Outlook中打开

①使用下面的.eml下载。在发送之前，替换所有[括号中的占位符]。

✉ 打开 Outlook (仅主题)

📎 下载 .eml 模板

TAC 10模板，支持PSIRT2a的IOC/它们确实重建(以前受影响)

使用案例

发送给其SD-WAN日志显示与PSIRT2a建议相关的危害表现(IoC)以及先前重建交换矩阵的客户的邮件。提供更新的补救指南，提供三个选项（选项2后续选项）。

主题

需要采取紧急行动：SD-WAN基础设施关键漏洞补救 — SR [SR#]

邮件

亲爱的用户：

感谢您联系思科技术支持中心(TAC)，了解服务请求[SR#]下最近的SD-WAN PSIRT建议。

在分析您的SD-WAN交换矩阵提供的日志后，我们的团队确定了2026年6月5日SD-WAN漏洞咨询相关的危害表现(IOC)。我们还知道，您的环境之前已进行了重建，这是与早期建议相关的补救步骤的一部分。

我们提供关键更新来补救您的SD-WAN交换矩阵，如[SR#]和之前传达的安全公告中所述。此更新特定于所提供日志显示危害表现(IOC)证据的交换矩阵。

虽然您之前选择了基于选项2（包括软件升级、控制器重新部署和SSH密钥轮换）的补救计划，但是我们对威胁形势的分析仍在继续发展。关于利用这些漏洞的新技术见解表明，强烈敦促采取其他措施，以降低持续存在的风险，并帮助确保证书信任链的完整性。

需执行的操作：

我们更新了推荐的补救策略，通过包含额外的根证书轮换来提供更全面的防御。

请注意，补救措施需要执行额外的维护活动，其中可能包括计划内网络停机时间。鉴于我们的首要任务是确保网络的安全性和完整性，我们制定了三种不同的补救方案。以下每个选项均提供运营影响与安全保证之间的平衡，供您考虑。由于您的内部风险状况是唯一的，思科无法推荐特定路径。

方案 A：通过滚动重启重新部署。通过避免网络停机来优先处理运营连续性，尽管它在过渡过程中仍存在威胁持久性的风险。

描述：涉及控制器重新部署，以及SSH密钥和证书轮换。在迁移期间，通过vManage连接现有控制器组件以部署新交换矩阵，并在设备迁移后立即删除每个控制器组件。

方案 B：通过硬切换重新部署。提供更高级别的安全保证。由于新控制器从未连接到旧控制器，因此存在完全隔离。由于所有设备都需要重新建立连接并交换路由/连接信息，因此这会对整体网络运营造成影响。中断时间将取决于站点数量、交换的前缀数量等。

描述：涉及控制器重新部署以及SSH密钥和证书轮换，但在重新部署期间，旧控制器组件与新交换矩阵隔离。

方案C：完全重建系统。通过建立干净的基线提供最高级别的安全保证，尽管这是最复杂的方法，并且在重建期间存在与配置相关的不稳定风险。这是一个漫长的选择，需要重建模板和策略数据库的专业知识。

在您的团队审查了这些选项并确定了与您的风险管理标准最相符的方法后，请回复此邮件通知我们。

收到您的选择后，我们将协调维护窗口，开始必要的技术准备以执行。

感谢您一如既往地专注于维护安全的网络基础设施。如果您需要通过回复此电子邮件或通过现有的服务请求进一步进行技术说明，请告知我们。

此致，
思科

在Outlook中打开

①使用下面的 .eml 下载。在发送之前，替换所有[括号中的占位符]。

✉ 打开Outlook (仅主题)

↓ 下载.eml模板

TAC 11模板，无适用于PSIRT2a的IOC/它们未重建(以前受到影响)

使用案例

发送给其SD-WAN日志未显示与PSIRT2a建议相关的危害表现(IoC)且未重建其交换矩阵的客户。提供更新的补救指南，提供三个选项（选项1后续选项）。

主题

需要采取紧急行动：SD-WAN基础设施关键漏洞补救 — SR [SR#]

邮件

亲爱的用户：

感谢您联系思科技术支持中心(TAC)，了解服务请求[SR#]下最近的SD-WAN PSIRT建议。

在查看从您的SD-WAN交换矩阵提供的日志和信息后，我们没有确定与2026年6月5日SD-WAN漏洞通知相关的危害表现(IoC)。

我们还知道，您的环境尚未根据之前的建议进行完全重建。思科建议查看以下更新的补救指南，以帮助降低潜在风险，并加强SD-WAN证书信任链的完整性。

考虑到这一点，我们提供关键更新来补救您的SD-WAN交换矩阵，如[SR#]和之前传达的安全公告中所述。

虽然您之前选择了基于选项1（结合软件升级和SSH密钥轮换）的补救计划，但我们对于威胁形势的

分析也在不断发展。关于利用这些漏洞的新技术见解表明，强烈敦促采取其他措施，以降低持续存在的风险，并帮助确保证书信任链的完整性。

需执行的操作：

我们更新了推荐的补救策略，通过包含额外的根证书轮换来提供更全面的防御。

请注意，补救措施需要执行额外的维护活动，其中可能包括计划内网络停机时间。鉴于我们的首要任务是确保网络的安全性和完整性，我们制定了三种不同的补救方案。以下每个选项均提供运营影响与安全保证之间的平衡，供您考虑。由于您的内部风险状况是唯一的，思科无法推荐特定路径。

方案 A：通过滚动重启重新部署。通过避免网络停机来优先处理运营连续性，尽管它在过渡过程中仍存在威胁持久性的风险。

描述：涉及控制器重新部署，以及SSH密钥和证书轮换。在迁移期间，通过vManage连接现有控制器组件以部署新交换矩阵，并在设备迁移后立即删除每个控制器组件。

方案 B：通过硬切换重新部署。提供更高级别的安全保证。由于新控制器从未连接到旧控制器，因此存在完全隔离。由于所有设备都需要重新建立连接并交换路由/连接信息，因此这会对整体网络运营造成影响。中断时间将取决于站点数量、交换的前缀数量等。

描述：涉及控制器重新部署以及SSH密钥和证书轮换，但在重新部署期间，旧控制器组件与新交换矩阵隔离。

方案C：完全重建系统。通过建立干净的基线提供最高级别的安全保证，尽管这是最复杂的方法，并且在重建期间存在与配置相关的不稳定风险。这是一个漫长的选择，需要重建模板和策略数据库的专业知识。

在您的团队审查了这些选项并确定了与您的风险管理标准最相符的方法后，请回复此邮件通知我们。收到您的选择后，我们将协调维护窗口，开始必要的技术准备以执行。

感谢您一如既往地专注于维护安全的网络基础设施。如果您需要通过回复此电子邮件或通过现有的服务请求进一步进行技术说明，请告知我们。

此致，
思科

在Outlook中打开

① 使用下面的 .eml 下载。在发送之前，替换所有 [括号中的占位符]。

✉ 打开 Outlook (仅主题)

↓ 下载 .eml 模板

TAC 12 Template for yes IOC for PSIRT2a/they not rebuild(PREVIOUSLY IMPACTED)。

使用案例

发送给其SD-WAN日志显示与PSIRT2a建议相关的危害表现(IoC)且未重建其交换矩阵的客户。提供更新的补救指南，提供三个选项（选项1后续选项）。

主题

需要采取紧急行动：SD-WAN基础设施关键漏洞补救 — SR [SR#]

邮件

亲爱的用户：

感谢您联系思科技术支持中心(TAC)，了解服务请求[SR#]下最近的SD-WAN PSIRT建议。

在分析您的SD-WAN交换矩阵提供的日志后，我们的团队确定了2026年6月5日SD-WAN漏洞咨询相关的危害表现(IoC)。此外，我们了解您的环境尚未根据之前的建议进行完全重建。

鉴于这些指标的存在和对威胁形势的不断了解，必须审核和实施下面概述的更新补救指南，以降低持续性风险并确保您的SD-WAN证书信任链的完整性。

我们提供关键更新来补救您的SD-WAN交换矩阵，如[SR#]和之前传达的安全公告中所述。此更新特定于所提供日志显示危害表现(IoC)证据的交换矩阵。

虽然您之前选择了基于选项1（结合软件升级和SSH密钥轮换）的补救计划，但我们对于威胁形势的分析也在不断发展。关于利用这些漏洞的新技术见解表明，强烈敦促采取其他措施，以降低持续存在的风险，并帮助确保证书信任链的完整性。

需执行的操作：

我们更新了推荐的补救策略，通过包含额外的根证书轮换来提供更全面的防御。

请注意，补救措施需要执行额外的维护活动，其中可能包括计划内网络停机时间。鉴于我们的首要任务是确保网络的安全性和完整性，我们制定了三种不同的补救方案。以下每个选项均提供运营影响与安全保证之间的平衡，供您考虑。由于您的内部风险状况是唯一的，思科无法推荐特定路径。

方案 A：通过滚动重启重新部署。通过避免网络停机来优先处理运营连续性，尽管它在过渡过程中仍存在威胁持久性的风险。

描述：涉及控制器重新部署，以及SSH密钥和证书轮换。在迁移期间，通过vManage连接现有控制器组件以部署新交换矩阵，并在设备迁移后立即删除每个控制器组件。

方案 B：通过硬切换重新部署。提供更高级别的安全保证。由于新控制器从未连接到旧控制器，因此存在完全隔离。由于所有设备都需要重新建立连接并交换路由/连接信息，因此这会对整体网络运营造成影响。中断时间将取决于站点数量、交换的前缀数量等。

描述:涉及控制器重新部署以及SSH密钥和证书轮换，但在重新部署期间，旧控制器组件与新交换矩阵隔离。

方案C:完全重建系统。通过建立干净的基线提供最高级别的安全保证，尽管这是最复杂的方法，并且在重建期间存在与配置相关的不稳定风险。这是一个漫长的选择，需要重建模板和策略数据库的专业知识。

在您的团队审查了这些选项并确定了与您的风险管理标准最相符的方法后，请回复此邮件通知我们。收到您的选择后，我们将协调维护窗口，开始必要的技术准备以执行。

感谢您一如既往地专注于维护安全的网络基础设施。如果您需要通过回复此电子邮件或通过现有的服务请求进一步进行技术说明，请告知我们。

此致，
思科

在Outlook中打开

①使用下面的 .eml 下载。在发送之前，替换所有[括号中的占位符]。

✉ 打开Outlook (仅主题)

↓ 下载.eml模板

新客户的WAVE 2A电邮 (之前未受影响)

TAC 13模板，无IOC/无可用的固定版本 (WAVE 2a — 等待修复)

使用案例

发送给其SD-WAN日志未显示与CVE-2026-20245相关的危害表现(IoC)，但其平台/版本当前没有固定软件版本的客户。建议客户应用临时强化措施并等待固定版本通知。

主题

更新：完成CVE-2026-20245的IoC评估 — 当前无固定版本 — SR [SR#]

邮件

亲爱的用户：

感谢您联系思科技术支持中心(TAC)，了解服务请求[SR#]下有关CVE-2026-20245的信息。

我们已经完成了对您从SD-WAN控制组件提供的管理技术文件的分析。在审核的日志中，我们没有发现与CVE-2026-20245相关的任何危害表现(IoC)。

请注意，根据[Cisco SD-WAN强化指南](#)^[1]在您的环境中配置的日志保留期，可能会限制为思科检索和为此审核提供的日志数据量。

重要信息 — 当前没有可用的固定软件版本：

目前，您的当前平台和软件版本没有可用的固定软件版本来修复此漏洞。思科工程部正在积极致力于提供固定版本。固定软件可用后，官方[安全咨询](#)^[2]将使用固定版本信息进行更新。

建议采取的临时措施：

在等待固定版本时，我们强烈建议实施以下强化措施来减少暴露情况：

1. 应用强化最佳实践：查看并实施[Cisco SD-WAN强化指南](#)^[1]中的建议以减少攻击面。
2. 监控安全建议：定期检查官方[安全建议](#)^[2]以了解您的平台固定版本可用性的更新。
3. 升级计划：立即开始升级计划，以便您准备在发布固定版本后立即执行升级。
4. 监控您的环境：继续监控您的SD-WAN控制组件，以发现任何异常行为或意外的配置更改。

后续方案

当固定软件版本可用时，我们将更新此案例。此时，您应优先处理所有SD-WAN控制组件（管理器、控制器、验证器）在可行的情况下尽快升级到固定版本。

如果您有BCS/LCS订用，请联系Cisco NCE或Delivery Manager获取有关升级规划的其他指导。

感谢您的耐心和对基础设施安全的承诺。如有任何疑问或需要进一步的协助，请尽快回复本案。

顺致敬意！

Cisco 技术支持中心 (TAC)

链接：

[1] [思科SD-WAN加固指南](#)

[2] [官方安全建议\(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

①发送前替换所有[带括号的占位符]。

✉打开Outlook (仅主题)

📄下载.eml模板

TAC 14模板，无可用的IOC/固定版本 (WAVE 2a — 立即升级)

使用案例

发送给其SD-WAN日志未显示与CVE-2026-20245相关的危害表现(IoC)且有固定软件版本的客户。建议客户立即继续进行升级规划和执行。

主题

更新：完成CVE-2026-20245的IoC评估 — 未找到IoC，需要升级 — SR [SR#]

邮件

亲爱的用户：

感谢您联系思科技术支持中心(TAC)，了解服务请求[SR#]下有关CVE-2026-20245的信息。

我们已经完成了对您从SD-WAN控制组件提供的管理技术文件的分析。在审核的日志中，我们没有发现与CVE-2026-20245相关的任何危害表现(IoC)。

请注意，根据[Cisco SD-WAN强化指南](#)^[1]在您的环境中配置的日志保留期，可能会限制为思科检索和为此审核提供的日志数据量。

重要信息 — 需要升级：

尽管未发现任何IoC，但底层漏洞仍然存在，直到您的SD-WAN控制组件升级到固定软件版本。您的平台现在可以使用固定版本。

请优先确定升级规划和执行的优先级，作为补救此漏洞的最关键步骤。如果您尚未安排此升级，请立即执行此操作。

后续方案

1. 升级所有SD-WAN控制组件：将您的经理(vManage)、控制器(vSmart)和验证器(vBond)升级到官方安全建议^[2]中列出的[固定软件版本](#)。
2. 升级资源：有关详细的升级说明，请参阅以下思科官方文档：
 - [开始Catalyst SD-WAN升级](#)^[3]
 - [思科SD-WAN升级指南](#)^[4]

3. 案例结束：成功完成整个环境的软件升级后，您可以考虑解决此问题并继续执行标准关闭过程。

如果您有BCS/LCS订用，请联系Cisco NCE或Delivery Manager获取有关升级过程的更多指导。

我们将继续监视您的案例。如果在10个工作日内没有收到回复，我们将假定无需进一步帮助，并继续进行正常的TAC案例解决程序。

顺致敬意！

Cisco 技术 支持 中心 (TAC)

链接：

[1]思科SD-WAN加固指南

[2]官方安全建议(cisco-sa-sdwan-privesc-4uxFrdzx)

[3]开始Catalyst SD-WAN升级

[4]思科SD-WAN升级指南

在Outlook中打开

① 发送前替换所有[带括号的占位符]。

✉ 打开 Outlook (仅主题)

📎 下载 .eml 模板

TAC 15模板，用于确定IOC/提供固定版本 (WAVE 2a — 紧急升级)

使用案例

发送给其SD-WAN日志显示与CVE-2026-20245相关的危害表现(IoC)且有固定软件版本的客户。建议客户紧急升级，并安排审查电话讨论结果和补救。

主题

紧急:已确定CVE-2026-20245的IoC — 需要立即升级 — SR [SR#]

邮件

亲爱的用户：

感谢您联系思科技术支持中心(TAC)，了解服务请求[SR#]下有关CVE-2026-20245的信息。

通过分析您的SD-WAN控制组件提供的管理技术文件，我们的团队已识别出与CVE-2026-20245相关的危害表现(IoC)。

鉴于这些调查结果的性质，我们必须尽快讨论技术细节和建议的后续步骤。我们希望与您的团队安排一次电话会议，以审查具体的调查结果并讨论适当的补救路径。

需要立即执行的操作：

1. **立即升级SD-WAN控制组件**：您的平台可使用固定软件版本。请尽快将您的经理(vManage)、控制器(vSmart)和验证器(vBond)升级到官方安全建议^[1]中列出的固定软件版本。升级会立即关闭漏洞。
2. **安排审核呼叫**：请在接下来的[例如4-8小时]内向我们提供简短电话来查看IoC调查结果并讨论建议的补救选项。
3. **应用强化最佳实践**：查看并实施[Cisco SD-WAN加固指南](#)^[2]中的建议，以在计划补救时缩小您的攻击面。

升级资源：

- [开始Catalyst SD-WAN升级](#)^[3]
- [思科SD-WAN升级指南](#)^[4]

重要信息：升级后，可能会建议其他补救步骤（例如控制器重新部署和证书轮换），具体取决于所识别威胁的严重程度。这些将在审核通话期间讨论。

有关详细的补救选项，另请参阅[TAC补救指南](#)^[5]。

我们的主要目标是帮助您保护环境和降低任何潜在风险。我们感谢您迅速关注此事，并期待与您协调。

顺致敬意！

Cisco 技术支持中心 (TAC)

链接：

[1] [官方安全建议\(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

[2] [思科SD-WAN加固指南](#)

[3] [开始Catalyst SD-WAN升级](#)

[4] [思科SD-WAN升级指南](#)

[5] [TAC补救指南](#)

在Outlook中打开

① 发送前替换所有[带括号的占位符]。

✉ 打开Outlook（仅主题）

📎 下载.eml模板

确定IOC的TAC 16模板/无可用的固定版本（WAVE 2a — 强化并等待修复）

使用案例

发送给其SD-WAN日志显示与CVE-2026-20245相关的危害表现(IoC)的客户，但这些客户当前没有为其平台/版本提供的固定软件版本。建议立即强化，安排审查呼叫，并通知客户他们必须等待固定版本才能完全修复。

主题

紧急:为CVE-2026-20245识别的IoC — 当前无固定版本 — SR [SR#]

邮件

亲爱的用户：

感谢您联系思科技术支持中心(TAC)，了解服务请求[SR#]下有关CVE-2026-20245的信息。

通过分析您的SD-WAN控制组件提供的管理技术文件，我们的团队已识别出与CVE-2026-20245相关的危害表现(IoC)。

鉴于这些调查结果的严重性，尽早讨论其中的技术细节以及建议采取的临时措施至关重要。我们希望与您的团队安排一次电话来审查具体调查结果。

重要信息 — 当前没有可用的固定软件版本：

目前，您的当前平台和软件版本没有可用的固定软件版本来完全修复此漏洞。思科工程部正在积极致力于提供固定版本。固定软件可用后，官方安全[咨询](#)^[1]将使用固定版本信息进行更新。

需要立即执行的操作：

1. **安排审核呼叫：**请告知您在未来[如4-8小时]内是否有时间参加简短的电话会议，以查看IoC调查结果并讨论临时遏制措施。
2. **立即应用强化最佳实践：**查看并实施[Cisco SD-WAN强化指南](#)^[2]中的建议，以缩短攻击面，同时等待固定版本。
3. **增强监控：**密切监控您的SD-WAN控制组件，以发现任何异常行为、意外配置更改或未经授权的访问尝试。
4. **监控安全建议：**定期检查官[方安全建议](#)^[1]以了解您的平台固定版本可用性的更新。
5. **升级计划：**立即开始升级计划，以便您准备在发布固定版本后立即执行升级。

后续方案

当固定软件版本可用时，我们将更新此案例。此时，您必须确定所有SD-WAN控制组件（管理器、控制器、验证器）立即升级到固定版本的优先级。升级后，将根据我们通话期间检查的结果讨论其他补救步骤（例如控制器重新部署和证书轮换）。

另请参阅[TAC补救指南](#)[3]，了解固定版本可用后将应用的补救选项的相关信息。

我们的主要目标是帮助您保护环境和降低任何潜在风险。我们感谢您迅速关注此事，并期待与您协调。

顺致敬意！

Cisco 技术支持中心 (TAC)

链接：

[1]官方[安全建议](#)([cisco-sa-sdwan-privesc-4uxFrdzx](#))

[2]思科[SD-WAN加固指南](#)

[3] TAC[补救指南](#)

在Outlook中打开

① 发送前替换所有[带括号的占位符]。

✉ 打开Outlook (仅主题)

↓ 下载.eml模板

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。