修复Catalyst SD-WAN安全建议 — 2026年9月

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

补救工作流程概述

步骤 1：从所有管理员收集管理技术文件

- 备选：手动验证（仅当无法收集管理技术时）

步骤 2：升级到固定软件版本

步骤 3：打开TAC案例并上传管理技术文件以进行扫描

步骤 4：如果确定存在危害 — TAC指南

固定软件版本

- 重要参考

附录：手动验证步骤（仅当无法进行管理技术收集时）

- 如何确定危害表现
- 验证1:审核服务代理访问日志
- 验证2:审核Manager服务器日志

常见问题解答

简介

本文档介绍根据PSIRT建议日期（2026年9月30日）识别和修复关键SD-WAN安全漏洞的步骤。思科强烈建议升级到固定软件版本以修复此问题。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Catalyst SD-WAN架构和控制组件（管理器、控制器和验证器）
- Cisco Catalyst SD-WAN升级过程
- Cisco TAC案例管理和管理技术收集流程

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

有关详细背景信息和最新更新，请参阅官方PSIRT咨询页面。

此建议可通过以下链接获得：

- Cisco Catalyst SD-WAN Manager API身份验证旁路漏洞(CVE-2026-76504、CWE-177)。 安全影响等级：关键（CVSS基础评分9.8）。

此PSIRT建议解决了以下缺陷：

- Cisco Bug ID CSCww79570

此建议会影响Cisco Catalyst SD-WAN Manager(vManage)。

补救工作流程概述



注意：运行早于第一个固定版本的所有SD-WAN Manager(vManage)都存在漏洞，需要立即升级。但是，并非所有Catalyst管理器都显示危害迹象。

所需操作：收集所有Catalyst SD-WAN管理器的管理技术，将所有技术升级到固定版本，并打开Cisco TAC案例，以便TAC可以扫描您的管理技术，查找危害表现。

TAC可用于：

- 扫描您提供的管理技术以发现危害表现
- 如果在升级过程中遇到问题，则提供升级支持
- 如果识别出危害表现，则指导您进行其他补救

1. 在升级之前，收集管理技术 — 在所有Catalyst SD-WAN管理器上运行admin-tech，包括群集和灾难恢复(DR)部署的每个节点，以确保不会丢失诊断数据。选择Log and Tech选项。核心不是必需的。
2. 升级到固定版本-将所有管理器(vManage)升级到固定软件版本表中列出的固定软件。升级之前不要等待TAC扫描结果。升级到固定版本是最高优先级并关闭漏洞。第3步中的TAC扫描确定升级后是否需要执行任何进一步的操作。
3. 打开TAC案例并上传管理技术以扫描危害表现 — 打开思科TAC案例并上传第1步中收集的所有管理技术日志捆绑包。TAC扫描管理技术以查找危害表现。
4. 如果确定存在危害，请使用TAC指南 — 如果TAC确定您的环境中的危害表现，请完成TAC提供的所有补救指南。如果未发现危害表现，则无需在升级后执行进一步操作。

步骤 1：从所有管理员收集管理技术文件

必需：在升级之前从所有管理器(vManage)收集管理技术文件，以确保不会丢失诊断数据。TAC在第3步使用这些文件扫描您的环境是否存在危害表现。

集合：

对于admin-tech generation，请选择Log and Tech options。核心不是必需的。

1. 在所有管理器上运行管理技术(vManage)。
2. 如果您的管理器作为集群运行，请对每个集群成员运行admin-tech。
3. 如果您部署了灾难恢复(DR)，请在主站点和灾难恢复站点的每个Manager上运行admin-tech。

收集SD-WAN环境中的管理技术并上传到TAC案例

TAC会分析这些文件以评估您的环境是否存在危害表现，并指导适当的补救路径。

备选：手动验证（仅当无法收集管理技术时）

对于无法共享管理技术文件的用户，可以使用手动验证步骤。这些步骤提供必须记录并与TAC共享的初步指标。

有关详细过程，请参阅本文档末尾的手动验证步骤部分。记录所有调查结果，并在支持案例中将其提供给TAC。

步骤 2：升级到固定软件版本

收集第1步中的管理技术后，将所有管理器(vManage)升级到固定软件版本。

⚠ 重要信息：升级之前不要等待TAC扫描结果。升级到固定版本是最高优先级并关闭漏洞。第3步中的TAC扫描确定升级后是否需要执行任何进一步操作。

从本文档的固定软件版本表中选择适当的版本。

警告：升级必须保持在当前主版本内。如果没有明确的TAC指导，请勿升级到更高的主要版本。

使用vManage GUI或CLI升级SD-WAN控制器

如果您在升级过程中遇到任何问题，请打开TAC案例以获得升级支持。

步骤 3：打开TAC案例并上传管理技术文件以进行扫描

在第2步升级后，打开Cisco TAC支持案例，并上传在第1步中收集的管理技术文件。TAC扫描管理技术以查找危害表现。

所需操作：

1. 打开标题中带有CVE-ID“CVE-2026-76504”的严重性3 TAC案例，以启动扫描过程。
2. 上传第1步中收集的所有管理技术日志捆绑包（所有管理器，包括群集和DR节点）。
3. 等待TAC完成扫描并传达结果。

TAC分析管理技术文件并传达扫描结果。如果未发现危害表现，则无需在升级后执行进一步操作。

步骤 4：如果确定存在危害 — TAC指南

如果TAC发现您的环境中存在危害表现，TAC会联系您提供具体的补救指导。完成TAC提供的所有说明。

如果没有发现危害表现，则步骤2中完成的升级就足够了，无需进一步补救。

固定软件版本

这些软件版本包含此漏洞的修补程序。升级到当前版本系列中的第一个固定版本。

Cisco Catalyst SD-WAN软件版本	第一个固定版本	可用软件
早于20.9[1]	迁移到固定版本。	
20.9	20.9.10.1	20.9.10.1 vManage升级映像
20.12	20.12.8.2	20.12.8.2 vManage升级映像
20.15	20.15.6.1	20.15.6.1 vManage升级映像
20.18	20.18.4.1	20.18.4.1 vManage升级映像
26.1	26.1.2.1	26.1.2.1 vManage升级映像
26.2	26.2.1	26.2.1 vManage升级映像

[1]这些版本已到达软件维护终止日期。思科强烈鼓励客户升级到支持的版本。

思科产品安全事件响应团队(PSIRT)仅验证建议中记录的受影响和固定版本信息。

思科还在基于云的思科SD-WAN云（思科托管）版本20.15.605中解决了此漏洞。无需用户操作。客户可使用服务GUI中的“帮助”(Help)功能确定当前补救状态或软件版本。

重要参考

- 升级表
- 控制器兼容性矩阵

附录：手动验证步骤（仅当无法进行管理技术收集时）

管理技术集合是首选和推荐的方法。如果您绝对无法收集和共享管理技术文件，请仅使用手动验证。如果无法收集管理技术文件，请使用以下手动步骤收集TAC的初步指标。

- 这些步骤仅提供初步数据
- 为了进行准确评估，强烈建议使用管理技术收集

- 记录您的调查结果，并在支持案例中与TAC共享这些结果
- TAC作出正式评估决定

要求:这些步骤必须在所有Manager(vManage)上执行，包括灾难恢复(DR)站点中的每个群集成员和每个Manager。从vshell（从Manager CLI访问vshell）访问日志文件，并查看当前和轮换的日志文件。

如何确定危害表现

此建议有两种危害表现。两者都与j_security_check的条目有关，其中请求的字符被编码（例如/%6a_security_check），来自未知或未经授权的IP地址。

⚠ 重要信息：本部分的示例说明在请求中使用%6a作为编码字符j。这只是一个示例，该漏洞允许使用请求中编码的任何一个字符。

Cisco Catalyst SD-WAN Manager系统暴露在互联网中，且端口暴露在互联网中，因此存在受到威胁的风险。在某些情况下，这些危害表现可能发生在标准操作期间。因此，必须根据正常的网络状况评估这些威胁，以识别并避免误报。

指示器	日志文件	含义	确认
收到编码的j_security_check请求	/var/log/nms/containers/service_proxy/serviceproxy-access.log*	客户端向Manager发送了此类请求。	验证1
已为viptela-reserved-*用户处理编码的j_security_check请求	/var/log/nms/vmanage-server.log*	Manager处理了针对视频保留 — *用户（保留的系统服务帐户）的此类请求。	验证2

验证1:审核服务代理访问日志

审核位于/var/log/nms/containers/service_proxy/serviceproxy-access.log的serviceproxy-access.log文件，查找与来自未知或未授权IP地址的j_security_check相关的条目，如下例所示：

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

vManage系统中的某些日志文件限制在根访问之后，客户无法直接访问。要查看这些日志，客户必须生成一个管理技术文件。

解释TAC的结果和文档

如果未找到此类条目：

- 在此管理器上未在此日志中检测到任何危害表现
- 记录您的TAC案例的结果
- 继续验证2，然后对其余管理器重复这两个验证

如果找到此类条目：

- 仔细检查显示的每个源IP地址
- 查找来自未知或未授权IP地址的条目。验证源IP是否属于环境中的授权活动（例如，您运行的漏洞扫描或渗透测试）
- 如果无法将源IP识别为合法，则这可能表示存在潜在危害表现
- 记录所有调查结果并立即打开TAC案例
- 在您的案例中包含日志条目、时间戳、源IP和HTTP状态代码
- TAC执行正式评估决定

验证2:审核Manager服务器日志

审核位于/var/log/nms/vmanage-server.log的vmanage-server.log文件，查找与来自未知或未经授权的IP地址的j_security_check相关的条目，特别是为包含以viptela-reserved — 开头的名称的用户调用的条目，如下所示：

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

Cisco Catalyst SD-WAN系统和接口配置指南的“身份验证、授权和记帐”部分中记录了病毒保留的系统服务帐户。

解释TAC的结果和文档

如果未找到此类条目：

- 在此管理器上未在此日志中检测到任何危害表现
- 记录您的TAC案例的结果
- 对其余Manager重复上述两种验证

如果找到此类条目：

- 这可能表示潜在的危害表现
- 记录所有调查结果并立即打开TAC案例
- 包括案例中的日志条目和时间戳，以及同一时间段的验证1结果
- TAC执行正式评估决定

常见问题解答

解决此安全建议的第一步是什么？

从所有管理器收集管理技术文件(vManage)，然后将所有管理器升级到固定软件版本。升级后，打开TAC案例并上传管理技术，以便TAC可以扫描您的环境是否存在危害表现。

哪些组件受此建议的影响？

仅影响Cisco Catalyst SD-WAN Manager(vManage)。

我们是否需要同时升级控制器、验证器或边缘路由器？

不，不是为了说明这个建议。将所有管理器(vManage)升级到固定版本，并使用控制器兼容性列表确认新的Manager版本与其他组件兼容。

是否有解决方法？

否。没有解决此漏洞的解决方法。升级到固定版本。

我需要升级到哪个版本？

尽快升级到当前版本系列中的第一个固定版本。请参阅本文档中的固定软件版本表。TAC会确认适合您特定环境的相应版本。

我已经升级到固定版本，以获取以前的SD-WAN安全建议。我是否需要再次升级？

是，除非当前版本等于或晚于“固定软件版本”(Fixed Software Versions)表格中的系列中的第一个固定版本。早期建议的固定版本不一定包含此漏洞的修复程序。

我是否需要从所有管理员收集管理技术人员？

Yes.TAC需要来自每个经理(vManage)的管理技术文件，包括灾难恢复(DR)站点中的每个群集成员和每个经理，以正确评估您的环境。

我可以自己检查危害表现吗？

Yes.如果无法收集管理技术文件，请在每个管理器上使用手动验证步骤，并与TAC共享结果。管理员技术收集仍然是首选方法，TAC会做出正式评估决定。

TAC如何确定我的系统是否已被入侵？

TAC使用专用工具分析管理技术文件，以评估您的环境是否存在危害表现。

如果确定了危害表现，将会发生什么情况？

TAC与您联系，讨论针对您的环境的后续步骤和指南。思科不会代表您执行补救 — TAC提供您继续操作所需的指导。

我能否在TAC分析我的管理技术之前开始升级？

Yes.收集管理技术，升级到固定版本，然后打开TAC案例，以便TAC可以扫描管理技术是否存在危害表现。

补救期间是否预计会停机？

影响取决于您的部署架构和补救路径。TAC提供有关在流程中最大限度地减少服务影响的指导。

我有云托管SD-WAN重叠。我的升级选项是什么？

对于云托管的重叠，客户有两种选择：

1. 导航到SSP >重叠详细信息>更改窗口，检查您的环境是否计划进行自动升级。
2. 如果您不想等待计划的升级，则有两个选项：
    - 使用本文档中提供的升级指南自行升级。
    - 打开备用TAC案例，以便获得首选维护窗口。如果您在升级过程中遇到困难，TAC会为您提供帮助。

我们是思科托管的重叠网络。我们是否需要检查SSP上的任何访问规则？

建议所有思科托管客户在SSP >重叠详细信息>允许入站规则中查看自己的允许入站规则，并确保仅允许来自您一方的必要前缀。这些规则仅适用于管理访问，不适用于边缘路由器。

Cisco TAC是否针对此漏洞提供调查分析或调查服务？

Cisco TAC可以通过扫描与该漏洞相关的危害表现(IoC)来帮助客户。但是，TAC不执行深入调查分析或事件调查。对于全面的调查分析工作或详细的安全调查，我们建议客户聘请首选的第三方事件响应(IR)公司。

针对我的SD-WAN重叠降低漏洞的一般最佳实践或方法是什么？

请参阅Cisco Catalyst SD-WAN加固指南，了解减少您的SD-WAN重叠中的漏洞的最佳实践和建议。

应该使用修复此建议的Manager(vManage)版本运行哪些控制器(vSmart)和验证器(vBond)版本？

此建议仅影响Cisco Catalyst SD-WAN Manager(vManage)，因此只有Manager会移至新版本。在“固定软件版本”(Fixed Software Versions)表中，将每个管理器升级到您的培训的第一个固定版本。

控制器和验证器不需要升级此建议:预期他们已运行Cisco Catalyst SD-WAN软件安全强化版本中发布的固定版本：2026年8月建议，同一系列中的版本是固定管理器版本的预期配对。

您的版本系列是您目前运行的主要版本系列，例如20.9、20.12、20.15、20.18、26.1或26.2。第一个固定版本是包含修复程序的同一系列中的最早版本，也是补救的最短、风险最低的路径，因为您仍然停留在已运行的系列中。您无需转移到较新的火车来解决此建议。如果您的经理已经达到或晚于您的培训第一个固定版本，它不会受到影响，并且不需要升级。只有低于20.9的版本才需要迁移到支持的系列，因为这些版本已到达软件维护终止日期。

使用常规升级流程和先前建议中使用的相同维护限制。唯一的更改是选择新的Manager映像。例如，在20.15系列中：

- 管理器(vManage)— 20.15.6.1
- 控制器(vSmart)和验证器(vBond)— 20.15.6

如果您的控制组件仍在2026年8月建议发布之前的版本上，请按照标准SD-WAN升级顺序从Manager开始。例如，如果您的组件在20.9.5上：

1. 将每个Manager(vManage)直接升级到修复此建议的版本，20.9系列中的20.9.10.1。
2. 将该系列的验证器(vBond)和控制器(vSmart)升级到2026年8月的固定版本，即20.9.10。

在本示例中，结束状态是Managers at 20.9.10.1和Validators and Controllers at 20.9.10。20.9版本仅作为示例显示；使用固定软件版本(Fixed Software Versions)表将相同的序列应用到运行的系列，以确定适合您的系列的正确Manager版本。

在哪里可以查看哪些控制器(vSmart)和验证器(vBond)版本与包含此修复程序的管理器(vManage)版本兼容？

使用控制器兼容性表。从固定软件版本表中查找要升级到的管理器版本，并确认其支持的控制器和验证程序版本。升级表显示到达该版本所支持的升级路径。

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）。