修复Catalyst SD-WAN安全建议 — 2026年6月

目录

简介

本文档介绍根据2026年6月4日PSIRT公告识别和解决SD-WAN中的关键安全漏洞的步骤。

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(vManage、vSmart、vBond)
- 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。

以下链接提供了以下建议：

- Cisco Catalyst SD-WAN Manager身份验证的权限提升漏洞

这些PSIRT建议解决了以下缺陷：

- 思科漏洞ID CSCwu18563

补救工作流程概述

此建议描述了SD-WAN Manager中需要网络管理员权限才能利用的权限提升漏洞。

根据建议，未经身份验证的远程攻击者获取这些权限的已知路径是利用CVE-2026-20182(cisco-sa-sdwan-rpa2-v69WY2SW)或CVE-2026-20127(cisco-sa-sdwan-rpa-EHchtZk)。

如果您的控制组件已针对这两种公告升级到固定版本，且思科在您为之前事件提供的管理技术文件中未发现任何潜在危害表现(IoC)，则基于所查看的文件，这些特定设备上会缓解此新漏洞的已知未经身份验证的攻击路径。

这并不能消除攻击者持有有效netadmin凭据的隐患。思科尚未发布针对此漏洞的软件修复程序，也没有可用的解决方法；进一步指导将随后提供。

所需操作：提交思科TAC案例以解决此安全建议。

TAC可用于：

- 评估您的环境是否有危害表现
- 根据评估指导您完成适当的补救路径
- 就确定危害表现之后需要采取的后续步骤提供指导

1. 收集管理技术 — 在所有控制组件(vSmart、vManage、vBond)上运行管理技术。vSmart管理技术不能同时运行 — 一次运行一个。其他所有信息都可以按任意顺序收集。选择Log and Tech选项。 核心不是必需的。
2. 打开TAC案例 — 联系思科TAC并提供所有控制组件管理技术日志捆绑包。
3. TAC评估 — 在您的环境中对危害表现进行初步评估，然后TAC在您的环境中对危害表现进行初步评估。
4. 执行补救 — 如果需要，完成TAC提供的特定流程。

步骤 1：从所有控制组件收集管理技术文件

必需：在任何升级或配置更改之前，从所有控制组件收集管理技术文件，以便保留诊断数据和任何

潜在危害表现(IoC)。TAC在第3步中使用这些文件分析您的环境。

集合：对于管理技术生成，请选择日志和技术选项(Log and Tech options)。核心不是必需的。

1. 在所有控制器上运行管理技术(vSmarts) — 不要同时运行这些控制器；一次收集一个
2. 在所有管理器上运行管理技术(vManagers)
3. 对所有验证程序运行管理技术(vBonds)

收集SD-WAN环境中的管理技术并上传到TAC案例

注意：TAC会分析这些文件以评估您的环境，以了解与此建议相关的危害表现。此咨询的分析侧重于特定日志条目，该日志条目不区分合法和恶意使用；需要由TAC进行手动审核。

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客户，可以使用手动验证步骤。此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：打开TAC案例并上传管理技术文件

在第1步中收集管理技术后，打开Cisco TAC支持案例，并上传收集的管理技术文件。TAC会分析管理员技术以寻找与此建议相关的危害表现。

所需操作：

1. 使用“CVE-2026-20245”和标题中的建议ID `cisco-sa-sdwan-privesc-4uxFrdzx`创建严重性3 TAC案例以启动分析。
2. 上传第1步（控制器、管理器和验证器）中收集的所有管理技术日志捆绑包。
3. 等待TAC完成分析并传达分析结果。

注意：思科尚未发布针对此漏洞的软件修复程序，也没有可用的解决方法。第3步中的TAC分析有助于确定您提供的管理技术文件中是否存在任何危害表现。在工程部门提供进一步指导后，将遵循该指南。

步骤 3：TAC评估

TAC对您在第2步中上传的管理技术文件执行初步分析，并评估它们是否有与此建议相关的危害表现

。

对于此建议，分析将重点放在`/var/log/scripts.log`中每个Manager(vManage)上的特定日志条目。由于基础命令是合法的，且日志不区分合法和恶意使用，因此任何匹配的条目都需要TAC针对客户的正常操作状态进行手动检查，然后才被视为已确认的指示符。

TAC分析的可能结果：

- 未标识匹配的日志条目 — 根据审核的管理技术文件，未发现与此建议关联的指示符。目前无需针对此建议采取进一步行动。结果仅限于收到的管理技术文件，可能受每台设备上的日志保留期的限制。
- 已识别匹配日志条目 — TAC将通过其他审核步骤吸引客户。由于思科尚未发布针对此建议的软件修复程序，因此仅升级并不能解决此漏洞。第4步中引用的相关TechZone文章中记录了针对已确认危害方案的TAC指南。

注意：根据建议，攻击此漏洞需要具有netadmin权限，未经身份验证的攻击者只能通过有效凭据或利用CVE-2026-20182或CVE-2026-20127来获取此权限。如果针对这两个建议将控制组件升级到固定版本，并且未针对之前事件识别出危害迹象，则基于所查看的文件，将在这些特定设备上缓解此新漏洞的已知未经身份验证的攻击路径。

步骤 4：如果确定危害表现 — 请遵循TAC指南

如果TAC发现您的环境中与此建议相关的危害表现，TAC会联系您并提供特定指导。完成TAC提供的所有说明。

如果没有为此建议确定危害表现，根据已审核的管理技术文件，目前无需针对此建议采取进一步措施。

重要信息：思科尚未发布此建议的软件修复程序，也没有可用的解决方法。由于攻击此漏洞需要通过CVE-2026-20182或CVE-2026-20127获取的netadmin权限，因此客户应确保完成这些先前建议的补救。有关已建立的补救流程，请参阅相应的文档：

考虑事项

在成功修复后，根据每个客户的特定安全保证要求，客户可能希望对下列安全防护活动进行评估并采取行动。无论选择哪个补救选项，这些活动都适用。它们由客户管理；思科不会代表客户指导或执行这些操作。

- 审核所有本地用户帐户
- 凭据轮换
- 设备配置中存在的所有机密信息的轮替，例如（非详尽列表）：

    - 本地用户帐户的凭据
    - SNMP 社区字符串
    - TACACS密钥
    - VPN预共享密钥和证书
    - 受信任的SSH密钥
- 审核配置模板

边缘设备 — 可疑危害

思科不建议使用特定补救路径；补救选项的选择取决于客户。作为客户评估其环境的参考说明：如果客户怀疑边缘设备受到危害，则受影响边缘设备的出厂重置和重新加入是客户在选择边缘设备时可能希望考虑的一项客户管理的操作。是否采用这种方法以及选择哪个选项取决于客户。

执行安全出厂重置的正确命令是：

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

固定软件版本

> ⚠ 重要信息：在本文档发布时，思科尚未发布解决CVE-2026-20245的软件修补程序。根据建议，思科计划在未来版本中解决Cisco Catalyst SD-WAN Manager中的此漏洞。没有变通办法。此部分将在固定软件可用时更新。

由于利用此漏洞需要未经身份验证的攻击者只能通过CVE-2026-20182或CVE-2026-20127获得的netadmin权限，因此鼓励客户确保其控制组件运行固定版本，以便满足这些之前的建议要求。2026年5月14日SD-WAN安全建议和相应的TechZone文档中记录了这些建议的固定版本：

- Cisco Catalyst SD-WAN控制器身份验证旁路漏洞（2026年5月14日）
- （固定软件版本表）

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）

> ✎ 注意：管理技术集合是首选方法。如果无法收集管理技术文件并与TAC共享，请仅使用下

面的手动验证步骤。该手动步骤的结果是初步的；记录调查结果并与TAC共享，TAC将执行正式评估。

注意：对于此建议，手动验证包括一次目标日志检查。搜索到的日志条目由legal命令生成，并且仅日志不能区分合法使用和恶意使用。任何匹配的条目都必须根据客户的正常运行状态进行检查，然后才能作为潜在指示符。如果匹配条目无法与正常操作协调，请记录发现结果并与TAC共享。

验证：在每台管理器(vManage)上检查`scripts.log`以获取租户列表上传条目

根据PSIRT建议，鼓励客户审计位于`/var/log/`的`scripts.log`文件，以查找与以下示例类似的条目：

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

步骤 1：访问每个Manager(vManage)上的vshell并搜索日志文件

在vManage CLI中，放入vshell并运行：

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

对部署中的每个vManage（包括所有集群成员和任何DR配对的vManage）重复此检查。

步骤 2：解释TAC的结果和文档

如果未返回匹配的条目：

- 在此设备上的日志文件中未发现与此建议相关的危害表现。
- 记录您的TAC案例的结果（包括设备主机名和搜索的日志文件的日期/范围）。
- 继续检查其余的Manager。

如果返回匹配的条目：

- 必须根据客户的正常运行状态检查每个匹配条目。基础命令（租户列表上传）是合法的，可能会在日常操作期间出现。
- 对于每个匹配条目，请捕获时间戳、完整日志行和after-cli路径引用的`文件路径`。
- 如果匹配条目无法与已知的合法操作协调，则这可能是一种危害表现。记录调查结果并将其提供给TAC以供审核。
- 记录所有调查结果并创建TAC案例。包括匹配的日志条目和source命令输出。
- TAC执行正式评估。如果评估发现危害表现，请遵循相关TechZone文档中所述的流程：和补

救指南。

常见问题解答

问:解决此安全建议的第一步是什么？

A：在任何升级或配置更改之前从所有控制组件(vSmart、vManage、vBond)收集管理技术文件，以保留诊断数据和任何潜在危害表现。然后打开思科TAC案例并上传管理技术，以便TAC可以分析它们。

问:思科是否已发布针对此漏洞的软件修复程序？

A：本文档发布时尚未提供。根据建议，思科计划在未来版本中解决Cisco Catalyst SD-WAN Manager中的此漏洞。没有变通办法。本文档将在固定版本可用时更新。

问:如果没有解决方法，思科为何建议立即采取任何措施？

A：利用此漏洞需要netadmin权限。根据建议，未经身份验证的攻击者只能通过有效凭据或通过利用CVE-2026-20182或CVE-2026-20127来获取这些权限。确保这些先前建议的控制组件升级到固定版本，从而解决了已知未经身份验证的路径来获取利用此漏洞所需的权限。第3步中的管理技术分析有助于确定所查看的文件中是否存在任何危害表现。

问:我是否需要从所有控制组件收集管理技术？

A：Yes.TAC需要所有控制器（vSmart，一次收集一个）、所有管理器(vManage)和所有验证器(vBond)的管理员技术文件来执行分析。

问:TAC如何确定我的系统是否有与此建议相关的危害表现？

A：TAC审核管理技术文件，并在每个管理器上查找`/var/log/scripts.log`中的PSIRT建议中所述的特定日志条目。基础命令是合法的；任何匹配的条目都必须根据您的正常运行状态进行检查，然后才能作为潜在指示符。TAC执行审核。

问:如果确定了危害表现，将会发生什么情况？

A：TAC会联系您并提供具体指导。由于此建议目前没有可用的软件修复程序，因此仅升级并不能解决已确认的危害。TAC的指导遵循了2026年5月和2026年2月公告的相关技术区文章中记录的流程。

问:边缘路由器(Cisco IOS XE)是否受此建议的影响？

A：此建议会影响Cisco Catalyst SD-WAN Manager。根据建议，思科观察到在有限的情况下，利用此漏洞导致配置更改推送到边缘设备；建议客户检验其边缘设备的配置。

问:哪些部署类型受到影响？

A：根据建议，无论设备配置如何，此漏洞都会影响所有Cisco Catalyst SD-WAN Manager部署类型，包括内部部署、Cisco SD-WAN Cloud-Pro、Cisco SD-WAN Cloud(Cisco Managed)和Cisco SD-WAN for Government(FedRAMP)。

问:我已经为2026年5月和2026年2月的公告进行了升级，没有为这些事件确定任何危害指标。我是否暴露在这种新的漏洞之下？

A：如果您的控制组件正在为CVE-2026-20182和CVE-2026-20127运行固定版本，并且所审核的管理技术文件中未发现之前事件的危害表现，则基于所审核的文件，可缓解这些特定设备上针对此新漏洞的已知未经身份验证的攻击路径。这并不能消除攻击者持有有效netadmin凭证的风险。

问:是否可以自己执行验证，而不是等待TAC?

A：无法共享管理技术的客户可以执行附录中描述的手动验证步骤。结果是初步的；记录调查结果并与TAC共享，TAC将执行正式评估。

问:强化SD-WAN重叠的一般最佳实践是什么？

A：有关最佳实践，请参阅Cisco Catalyst SD-WAN加固指南。

问:Cisco TAC是否针对此漏洞提供调查分析或调查服务？

A：思科TAC可以通过查看PSIRT建议中记录的危害表现的管理技术文件来帮助客户。思科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，我们鼓励客户与其首选的第三方事件响应(IR)公司接洽。

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）。