修复Catalyst SD-WAN安全建议 — 2026年6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：从所有控制组件收集管理技术文件

- 备选：手动验证（仅当无法收集管理技术时）

步骤 2：打开TAC案例并上传管理技术文件

步骤 3：TAC评估

步骤 4：如果确定危害表现 — 遵守TAC指南

固定软件版本

考虑事项

- 边缘设备 — 可疑危害

附录：手动验证步骤（仅当无法进行管理技术收集时）

- 验证CVE-2026-20245:在文件上传条目的每个控制组件上检查scripts.log
- 验证CVE-2026-20262:检查每个管理器上的日志文件(vManage)，了解任意文件写入条目

常见问题解答

简介

本文档介绍根据2026年6月4日和15日的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 Controller、Catalyst SD-WAN Manager和Catalyst SD-WAN Validator Authenticated权限提升漏洞
- Cisco Catalyst SD-WAN Manager任意文件写入漏洞

这些PSIRT建议解决了以下缺陷：

- Cisco Bug ID CSCwu18563
- Cisco Bug ID CSCwu18441

补救工作流程概述

以下建议描述了Cisco Catalyst SD-WAN中的两个漏洞。第一个(CVE-2026-20245)是SD-WAN控制组件中需要网络管理员权限才能利用的权限提升漏洞。第二个(CVE-2026-20262)是SD-WAN Manager(vManage)中的任意文件写入漏洞，允许经过身份验证的用户在受影响系统的文件系统上创建或覆盖任何文件。

对于CVE-2026-20245和CVE-2026-20262，未经身份验证的远程攻击者获取所需凭据的已知路径是利用CVE-2026-20182(cisco-sa-sdwan-rpa2-v69WY2SW)或CVE-2026-20127(cisco-sa-sdwan-rpa-EHchtZk)。CVE-2026-20245需要netadmin权限才能利用此漏洞，而CVE-2026-20262至少需要一个较低权限的单任务用户帐户。

如果您的控制组件已升级到固定版本，并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，可缓解这些特定设备上CVE-2026-20245和CVE-2026-20262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凭据的隐患。对于这两种建议，思科建议您升级到固定版本。

所需操作：打开思科TAC案例以解决这些安全建议。

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要采取的步骤提供指导

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- TAC根据提供的管理技术文件对环境中的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)

在SD-WAN环境中收集管理技术并上传到TAC案例



注意：TAC会分析这些文件以评估您的环境，以了解与这两种建议相关的危害表现。对于权限提升建议，分析重点是/var/log/scripts.log中的特定日志条目，该条目不区分合法使用和恶意使用；需要由TAC进行手动审核。对于任意文件写入建议，分析重点是/var/log/nms/vmanage-server.log中的条目；这些条目也可在标准操作期间发生，必须根据正常操作状态进行评估以避免误报。

备选：手动验证（仅当无法收集管理技术时）

如果无法共享admin-tech文件，则可以执行手动验证步骤。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会分析管理技术以获取与两个建议（CVE-2026-20245和CVE-2026-20262）相关的危害表现。

所需操作：

1. 使用“CVE-2026-20245, CVE-2026-20262”和标题中的建议ID `cisco-sa-sdwan-privesc-4uxFrdzx`和`cisco-sa-sdwan-arbfw-c2rZvQ`打开严重性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：目前，思科已在所有版本系列上发布了针对这些漏洞的软件修复程序，但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。升级到固定软件版本，并遵守TAC关于任何其他必要后续步骤的指导。

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，并评估与两个建议（CVE-2026-20245和CVE-2026-20262）相关的危害表现。

对于建议CVE-2026-20245，此分析侧重于每个控制组件（vManage、vSmart和vBond）上/var/log/scripts.log中的特定日志条目。 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根据您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。

对于建议CVE-2026-20262，此分析侧重于每个Manager(vManage)的/var/log/nms目录中的几个文件。在某些情况下，这些危害表现可能会在标准操作期间出现。

这些日志不区分合法和恶意使用；因此，任何匹配的条目需要先由TAC根据您的正常运行状态进行手动审核，然后才能作为确认的指示符。

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，未发现与任一建议相关的指示符。目前无需针对这些建议采取进一步的操作。结果仅限于收到的管理技术文件，并受每台设备上的日志保留期的限制。
- 识别匹配的日志条目 — TAC通过额外的审核步骤吸引用户。对于这两种建议，建议升级到固定版本。由于建议性质，可能还需要采取其他操作。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CVE-2026-20245建议，利用漏洞需要netadmin权限，而CVE-2026-20262至少需要较低权限的单任务用户帐户。未经身份验证的攻击者可以通过有效凭据或利用CVE-2026-20182或CVE-2026-20127来获取这些凭据。如果您的控制组件已升级到固定版本，并且未针对以前的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CVE-2026-20245和CVE-2026-20262的已知未经身份验证的利用路径。

步骤 4：如果确定危害表现 — 遵守TAC指南

如果TAC识别出与您环境中的这些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。

如果两个建议均未确定危害表现，则根据审核的管理技术文件，此时无需针对危害评估采取进一步措施。仍然强烈建议升级为两个建议的一个固定版本。

固定软件版本

这些软件版本包含已识别漏洞的修复程序：

应用于当前版本	固定版本	可用软件
20.9.9.1及更低版本	20.9.9.2	20.9.9.2适用于vManage、vSmart和vBond的升级映像
20.12.7.1及更低版本	20.12.7.2	20.12.7.2 vManage、vSmart和vBond升级映像
20.15.4.4及更低版本	20.15.4.5	20.15.4.5 vManage、vSmart和vBond升级映像
20.15.5.2及更低版本	20.15.5.3	20.15.5.3 vManage、vSmart和vBond升级映像
20.16、20.17、20.18.x	20.18.3.1	20.18.3.1 vManage、vSmart和vBond升级映像
26.1	26.1.1.2	26.1.1.2 vManage、vSmart和vBond升级映像

注意：对于CDCS（思科托管群集）上的客户，20.15.507也是固定版本。这特别适用于思科托管的集群部署，并且与标准升级路径分开处理。

重要参考：

- 升级表
- 控制器兼容性矩阵
- 修复Catalyst SD-WAN安全建议 — 2026年5月
- 修复Catalyst SD-WAN安全建议 — 2026年2月
- Cisco Catalyst SD-WAN控制器身份验证旁路漏洞（2026年5月14日）

考虑事项

在成功修复后，根据您的具体安全保证要求，思科建议您评估并处理此处列出的安全防护活动。无论选择哪个补救选项，这些活动都适用。它们是用户管理的；思科不会代表您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每个客户。



注意：在怀疑边缘设备受到危害时，在选择时，需要考虑客户管理的操作，即对受影响的边缘设备执行出厂重置和重新装入。是否采用这种方法以及选择哪个选项取决于每个客户。

执行安全出厂重置的正确命令是：

```
factory-reset all secure
```

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，请仅使用此处显示的手动验证步骤。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：对于这两个建议，手动验证包括目标日志检查。这些检查所针对的日志条目由合法命令和活动生成，而日志本身无法区分合法和恶意使用。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。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CVE-2026-20245:在文件上传条目的每个控制组件上检查`scripts.log`

根据PSIRT建议，建议用户审核日志文件中类似这些示例的条目。在20.9版及更高版本中，可在`scripts.log`的`/var/log/`中找到这些条目。在20.9之前的版本中，可以在`/var/log/tmplog/`上的`vdebug`日志中找到等效数据。

三个不同的合法上传命令在同一日志中以相同格式生成条目。必须对每个项目进行审计：

租户列表上传的示例条目 — vconfd_script_upload_tenant_list.sh:

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

vSmart序列号上载的示例条目 — vconfd_script_upload_vsmart_serial_numbers.sh:

```
Jun  5 13:06:39 Manager vScript: vSmart upload serial numbers: /usr/bin/vconfd_script_upload_vsmart_ser
```

ZTP机箱编号上传的示例条目 — vconfd_script_upload_chassis_number_file.sh:

```
Jun  5 13:08:47 Validator vScript: ZTP upload chassis numbers: /usr/bin/vconfd_script_upload_chassis_nu
```

步骤 1：访问每个控制组件上的vshell，并搜索适当的日志文件以查找CVE-2026-20245指标

日志文件位置取决于控制组件上运行的软件版本。在运行搜索之前确定哪项适用于您的环境。

下面的搜索命令使用加宽模式vconfd_script_upload_.*\.sh，因此每个日志位置的单个调用将捕获上述所有三个上载脚本（vconfd_script_upload_tenant_list.sh、vconfd_script_upload_vsmart_serial_numbers.sh和vconfd_script_upload_chassis_number_file.sh）。

版本20.9及更高版本 — **在/var/log/tmplog/中搜索scripts.log**:

在vManage CLI中，放入vshell并运行：

```
vs
zgrep -E "vconfd_script_upload_.*\.sh" /var/log/scripts.log*
```

20.9之前的版本 — 在/var/log/tmplog/中搜索**vdebug**日志：

在20.9之前的版本中，scripts.log不存在。等效日志数据写入/var/log/tmplog/vdebug。最多保留五个滚动编号文件（vdebug、vdebug.1至vdebug.5）。 搜索所有活动文件：

```
vs
zgrep -E "vconfd_script_upload_.*\.sh" /var/log/tmplog/vdebug*
```

除了活动文件以外，旧日志使用命名模式vdebug_<timestamp>.tar.gz在/var/log/中作为压缩的tar文件

存档，日志数据存储在存档中，位于var/log/tmplog。搜索所有存档：

```
for f in /var/log/vdebug_*.tar.gz; do echo "=== $f ==="; tar -xOf "$f" var/log/tmplog 2>/dev/null | gre
```

对部署中的每个控制组件（包括所有集群成员以及任何DR配对的vManage）重复所有适用的检查。

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：

- 必须根据您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、vSmart序列号上传和ZTP机箱号上传）是合法的，在日常操作期间显示。
- 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，则这是潜在的危害表现。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，请参阅相关TechZone文档中所述的流程：和补救指南。

验证CVE-2026-20262:检查每个管理器上的日志文件(vManage)，了解任意文件写入条目

根据PSIRT建议，建议用户在每个Manager(vManage)上审核这些日志文件，以查找类似于以下示例的条目：

vmanage-server.log中的可疑条目示例（位于/var/log/nms/）

```
11-June-2026 03:53:37,310 EDT INFO  [a66cdc5f-807d-4c23-944e-5c809a2ece6b] [server] [SdraAnyConnectFile
```

vmanage-appserver.log中的可疑条目示例（位于/var/log/nms/）

```
11-June-2026 07:52:55,275 UTC INFO  [server] (DeploymentScanner-threads - 2) WFLYSRV0010: Deployed "sus
```

serviceproxy-access.log中的可疑条目示例（位于/var/log/nms/containers/service-proxy/）

```
POST /suspicious/index.jsp HTTP/1.1
```



注意：在20.9之前的版本中，serviceproxy-access.log位于/var/log/nms/，而不是/var/log/nms/containers/service-proxy/。

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

从vManage CLI中，放入vshell并运行：

```
vs
zgrep "SdraAnyConnectFileUploadHandler" /var/log/nms/vmanage-server.log*
zgrep "WFLYSRV0010" /var/log/nms/vmanage-appserver.log*
```

在某些版本中，可以从vshell直接访问服务代理日志。在需要根外壳访问的版本上，下载admin-tech并使用与以下内容类似的命令以相同的方式搜索其中的文件serviceproxy-access.log:

20.9及更高版本：

```
tar -xOf

      .tar.gz var/log/nms/containers/service-proxy/serviceproxy-access.log 2>/dev/null | grep "suspicio
```

20.9之前的版本：

```
tar -xOf

      .tar.gz var/log/nms/serverproxy-access.log 2>/dev/null | grep "suspicious"
```

如果直接从vshell访问，请使用从前面两个命令的结果中识别的.war文件名（不带扩展名）代替suspicious:

20.9及更高版本：

```
zgrep "POST" /var/log/nms/containers/service-proxy/serviceproxy-access.log* | grep "suspicious"
```

20.9之前的版本：

```
zgrep "POST" /var/log/nms/serverproxy-access.log* | grep "suspicious"
```

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：

- 必须根据您的正常运行状态检查每个匹配条目。这些条目可以在标准操作期间出现，并且不会自行确认危害。
- 对于`vmanage-server.log`中的每个匹配条目，捕获上载处理程序中引用的时间戳、完整日志行和文件路径。
- 如果匹配条目无法与已知的合法操作协调，则这是潜在的危害表现。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，请参阅相关TechZone文档中所述的流程：和补救指南。

常见问题解答

问:解决这些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这些漏洞的软件修复程序？

A：是，两个建议都可使用固定版本，如固定软件版本部分中所列。没有变通办法。

问:为什么思科建议采取升级以外的措施？

A：利用这些漏洞需要经过身份验证的用户。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来获取这些凭据。确保将控制组件升级到这些先前建议的固定版本，从而解决了已知未经身份验证的路径，以获取利用这些漏洞所需的权限。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具有与这些建议相关的危害表现？

A：TAC会审核管理技术文件，以了解特定于每个咨询的危害表现。对于权限提升建议(CVE-2026-20245),TAC在`/var/log/scripts.log`中查找每个控制组件上的特定日志条目。对于任意文件写入建议(CVE-2026-20262),TAC会在每个Manager上的三个日志文件中查找特定的日志条目：、`/var/log/nms/vmanage-appserver.log`和`/var/log/nms/containers/service-proxy/serviceproxy-access.log`。在这两种情况下，底层活动都可能发生在标准操作期间；任何匹配的条目都会由TAC根据您的正常运行状态进行审核，然后作为确认的指示符。

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。仅升级并不能解决已确认的危害。TAC的指南基于TechZone相关文章中记录的2026年5月和2026年2月公告流程。

问:边缘路由器(Cisco IOS XE)是否受这些建议的影响？

A：这些建议主要影响Cisco Catalyst SD-WAN控制组件。对于权限提升建议(CVE-2026-20245)，所有控制组件(vManage、vSmart、vBond)都会受到影响，并且思科已观察到有限的情况，即利用漏洞导致配置更改推送到边缘设备；建议用户验证其边缘设备的配置。对于任意文件写入建议(CVE-2026-20262)，该漏洞仅限于SD-WAN Manager文件系统，并且不会直接影响边缘设备。

问:哪些部署类型受到影响？

A：根据这些建议，这些漏洞会影响所有Cisco Catalyst SD-WAN部署类型，无论设备配置如何，包括内部部署、Cisco SD-WAN Cloud-Pro、Cisco SD-WAN Cloud（思科托管）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。我是否接触到了这些新的漏洞？

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，将缓解这些特定设备上CVE-2026-20245和CVE-2026-20262的已知未经身份验证的利用路径。这并不能消除攻击者持有有效凭据的隐患。思科建议您针对这些建议升级到固定版本。

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用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是否为这些漏洞提供调查分析或调查服务？

A：思科TAC可以通过查看管理技术文件来协助用户，了解两个PSIRT建议中记录的危害表现。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，我们鼓励用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）。