修复Catalyst SD-WAN安全建议 — 2026年5月

目录

简介

本文档介绍根据2026年5月14日发布的PSIRT公告识别和修复SD-WAN中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控制器身份验证旁路漏洞
- Cisco Catalyst SD-WAN漏洞

这些PSIRT建议解决了以下缺陷：

- Cisco Bug ID CSCwt50498
- Cisco Bug ID CSCwt38739
- Cisco Bug ID CSCwt38767
- Cisco Bug ID CSCwt55544

补救工作流程概述

注意：所有SD-WAN控制器和管理器都存在漏洞，需要立即升级所有控制组件。但是，并非所有控制器都显示危害迹象。

所需操作：收集管理技术，升级到固定版本，然后打开思科TAC案例，以便TAC可以扫描您的管理技术是否存在危害表现。

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. 收集管理技术 — 在升级之前对所有控制组件(vSmart、vManage、vBond)运行管理技术，以确保不会丢失诊断数据。选择“日志”和“技术”选项。 核心不是必需的。

   警告：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

   ---

2. 升级到固定版本 — 将所有SD-WAN控制组件(vManage、vSmart、vBond)升级到“固定软件版本”(Fixed Software Versions)表中列出的固定软件版本。

   注意：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，请遵循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：从所有控制组件收集管理技术文件

必需：在升级之前从所有控制组件收集管理技术文件，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：

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

1. 在所有控制器(vSmarts)上运行管理技术 — 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)

注意：vSmart管理技术不能同时运行 — 一次收集一个。可以按任意顺序收集管理员和验证程序的管理技术。

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。

有关详细步骤，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SD-WAN控制组件（vManage、vSmart和vBond）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

✎ 注意：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. 使用“CVE-2026-20182”和标题中的相关PSIRT ID打开严重性3 TAC案例，以启动扫描流程。
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完成扫描并传达结果

✎ 注意：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 — 请遵循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
20.3、20.6 和 20.9	20.9.9.1	20.9.9.1适用于vManage、vSmart和vBond的升级映像
20.10、20.11、20.12.5及更早版本	20.12.5.4	20.12.5.4 vManage、vSmart和vBond升级映像
20.12.6.x	20.12.6.2	20.12.6.2 vManage、vSmart和vBond升级映像
20.12.7	20.12.7.1	20.12.7.1 vManage、vSmart和vBond升级映像
20.15、20.13、20.14、20.15.4.3及更早版本	20.15.4.4	20.15.4.4 vManage、vSmart和vBond升级映像
20.15.5.x	20.15.5.2	20.15.5.2 vManage、vSmart和vBond升级映像
20.16、20.17、20.18.x	20.18.2.2	20.18.2.2 vManage、vSmart和vBond升级映像

注：对于SD-WAN云（以前称为云交付Cisco Catalyst SD-WAN [CDCS]）上的客户，20.15.506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。所有此类客户都已升级到固定版本20.15.506。

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。

注意：

- 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:必须在所有控制组件上执行这些步骤。

验证1:在身份验证日志中检查未授权的SSH登录

步骤 1：确定有效的vManage系统IP

访问每个vSmart控制器并执行：

```
west-vsmart# show control connections | inc "vmanage|PEER|IP"
```

示例输出：

```
                                                PEER
      PEER  PEER  PEER            SITE       DOMAIN  PRIV    PEER                                PUB
INDEX TYPE  PROT  SYSTEM IP       ID         ID      PRIVATE IP                          PORT    PUBLIC I
-------------------------------------------------------------------------------------------------------
0     vmanage dtls 10.1.0.18     101018     0       10.1.10.18                          12346   10.1.10.1
```

步骤 2：构建正则表达式字符串（仅限vBond和vSmart）

将第1步中的所有系统IP合并为OR regex模式：

```
system-ip1|system-ip2|...|system-ipn
```

步骤 2b：vManage系统的附加步骤

如果在vManage自身上运行这些命令，请将本地主机IP(127.0.0.1)、本地系统IP、所有集群IP和VPN 0传输接口IP附加到正则表达式：

```
system-ip1|system-ip2|...|system-ipn|127.0.0.1|
```

要查找本地vManage系统IP，请使用：

```
show control local-properties
```

要查找VPN 0传输接口IP和集群IP，请使用：

```
show interface | tab
```

步骤 3：执行验证命令

运行此命令，用第2步中的regex字符串替换REGEX:

```
west-vsmart# vs
west-vsmart:~$ zgrep "Accepted publickey for vmanage-admin from " /var/log/auth.log* | grep -vE "\s(REG
```

注意：此命令过滤身份验证日志以仅显示来自意外来源的vmanage-admin登录。合法登录必须仅来自vManage相关IP。

步骤 4：解释TAC的结果和文档

如果未显示输出：

- 在此设备上未检测到危害表现
- 记录您的TAC案例的结果
- 继续评估其余控制器

如果打印日志行：

- 仔细检查所示的每个IP地址
- 验证IP与vManage基础设施（集群IP、旧系统IP或类似设备）无关
- 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
- 日志条目显示时间戳和源IP地址
- 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、时间戳和源IP
- TAC执行正式评估决定

验证2:检查控制器系统日志中的未授权对等连接

此命令从控制器系统日志文件中提取所有对等类型和对等系统ip对，并将其输出为列表供您查看。它不会自动标记可疑条目 — 您必须检查输出并确定每个对等系统IP是否是SD-WAN基础设施的已知合法部分。在所有控制组件（控制器、管理器和验证器）上运行此命令。

步骤 1：在每个控制组件上运行命令：

首先，访问vshell并导航到日志目录：

```
vs
cd /var/log
```

然后运行此命令搜索vsyslog*文件glob:

```
awk '{
  match($0, /peer-type:([a-zA-Z0-9]+)[^ ]* peer-system-ip:([0-9.:]+)/, arr);
  if(arr[1] && arr[2]) print "(" arr[1] ", " arr[2] ")";
}' vsyslog* | sort | uniq
```

对messages* file glob和vdebug*file glob重复此操作。

步骤 2：解释TAC的结果和文档

如果输出仅显示已知的vManage/vSmart/vBond系统IP:

- 未从此检查中检测到任何危害表现
- 记录您的TAC案例的结果
- 继续评估其余控制组件

如果输出包含无法识别的对等系统IP:

- 仔细检查显示的每个IP地址和对等体类型
- 验证IP与您的已知SD-WAN控制平面基础设施无关
- 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
- 在您的案例中包括peer-type和peer-system-ip对的完整命令输出
- TAC执行正式评估决定

验证3:检查活动控制连接上缺少质询确认

此检查会检查报告为活动（或最近断开）但缺少预期的质询 — 确认交换的对等会话的控制连接详细信息输出。在Tx或Rx统计信息中显示challenge-ack 0时，双向交换hello数据包的会话表示对等设备从未完成预期的挑战握手，即需要调查的异常。在所有控制组件（控制器、管理器和验证器）上运行此

命令。

步骤 1：收集控制连接详细信息输出

从设备CLI运行：

```
show control connections detail
show control connections-history detail
```

将输出保存到文件(例如vdaemon.txt)以供检查。

步骤 2：查找内容

对于每个对等记录(以REMOTE-COLOR- / SYSTEM-IP-标头分隔)，如果以下所有条件都为真，则标记该记录：

- 会话状态为UP或TEAR_DOWN
- Tx Statistics hello计数器和Rx Statistics hello计数器均非零（hello在两个方向上流动）
- challenge-ack在Tx Statistics或Rx Statistics块中为0(或两者)

匹配记录示例(请注意<<<箭头，突出显示缺少的质询 — ack)

```
-------------------------------------------------------------------------------------------
 REMOTE-COLOR- default SYSTEM-IP- 10.2.2.2   PEER-PERSONALITY- vmanage
-------------------------------------------------------------------------------------------
site-id             432567
domain-id           0
protocol            dtls
private-ip          10.0.0.1
private-port        12346
public-ip           192.168.1.1
public-port         50825
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:16:58
hello interval      1000
hello tolerance     12000

  Tx Statistics-
  --------------
    hello                   3423293
    challenge               1
    challenge-response      0
    challenge-ack           0           <<<< MISSING challenge-ack (Tx)
    ...

  Rx Statistics-
  --------------
    hello                   3423291
    challenge               0
    challenge-response      1
    challenge-ack           0           <<<< MISSING challenge-ack (Rx)
    ...
```

在上面的示例中，Tx和Rx hello计数器均为非零（活动连接），但challenge-ack在两个方向上均为0。

步骤 3：手动搜索命令

要快速显示已保存的vdaemon.txt(或包含show control connections detail输出的任何文件)中的候选记录，请运行：

```
grep -A20 'SYSTEM-IP' vdaemon.txt | grep -B5 'challenge-ack  0'
```

返回的每个块代表一个对等会话，其中质询ack报告为0。请完整查看每个块以确认状态为up或teardown_down，并且Tx和Rx中的hello计数器在将其视为命中之前为非零。

步骤 4：解释TAC的结果和文档

如果没有满足所有三个条件的记录：

- 未从此检查中检测到任何危害表现
- 记录您的TAC案例的结果
- 继续评估其余控制组件

如果一个或多个记录满足所有三个条件：

- 仔细检查每个标记记录的SYSTEM-IP-、private-ip和public-ip值
- 验证对等体不是SD-WAN控制平面中已知的合法部分（集群成员、DR站点、以前分配给组件的IP地址）
- 如果无法识别对等体是合法的，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
- 在您的案例中包含完全匹配的对等记录和source命令输出
- TAC执行正式评估决定

常见问题解答

问:解决此安全建议的第一步是什么？

A：从所有控制组件收集管理技术文件，然后将所有控制组件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。

问：我需要升级到哪个版本？

A.请尽早升级到最近的固定版本。

问:我是否需要从所有控制组件收集管理技术？

A：是，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)的管理员技术文件才能正确评估您的环境。

问:TAC如何确定我的系统是否已被入侵？

A：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。

问:是否有办法使用TAC工具执行自己的自动扫描？

A：客户还可以使用Cisco Bug ID CSCwt50498的Bug Search Tool页面上内置的自助"Check Bug Applicability"（检查Bug适用性）工具，从控制组件重新扫描管理技术。

问:如果确定了危害表现，将会发生什么情况？

A：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。

问:如何知道使用哪个固定软件版本？

A：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。

问:我能否在TAC分析我的管理技术之前开始升级？

A：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。

问:补救期间是否预计会停机？

A：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。

问:如果找不到危害表现，是否需要升级所有控制器？

A：是的，所有SD-WAN控制组件（vManage、vSmart和vBond）都必须升级到固定软件版本。仅升级一部分控制器是不够的。

问:我有云托管SD-WAN重叠。我的升级选项是什么？

A：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。

问:我们是否需要同时升级边缘路由器？

A：否，Cisco IOS XE设备不受此建议的影响。

问：我们是思科托管的重叠网络。我们是否需要修复任何ACL或对SSP采取措施？

A：建议所有思科托管的客户查看他们自己的在SSP上看到的允许入站规则，并确保仅允许来自您一侧的必要前缀。这些规则仅适用于管理访问，并且不适用于边缘路由器。请在SSP >重叠详细信息>允许入站规则中查看这些规则。请注意，思科在第0天从外部向云托管控制器进行调配时，端口22、830始终被默认阻止。

问:我们处于SD-WAN云（以前称为云交付的Cisco Catalyst SD-WAN [CDCS]）上。 我们将升级到哪个版本？

A：根据当前版本，SD-WAN云集群目前正在按计划进行升级或已经升级到固定版本。以下是SD-WAN Cloud（以前称为CDCS）固定版本：

1.早期采用者集群= 20.18.2.2（这实际上与标准版本相同）

2.建议版本集群= 20.15.506（带PSIRT修复的CDCS特定版本）

SD-WAN云客户无需采取任何有效措施来解决此PSIRT。

问:我们在共享租户上。我们将升级到哪个版本？

A：根据当前版本，共享租户当前按计划进行升级或已经升级到固定版本。以下是共享租户固定版本：

1.建议版本集群= 20.15.5.2

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可以通过扫描与这些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。

问: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？

A：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。

问:我们会在系统中看到来自“根”用户的日志。 这有关系吗？

A：检查系统当时还发生了什么情况。 这些日志完全可以预期。 例如，在生成admin-techs时，会看到来自“root”用户的系统登录更改日志。 在重新启动期间，也可以从“root”用户查看日志。

```
Feb 28 23:03:44 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-

       user-name:"root" user-id:245  generated-at:2-28-2026T23:3:44

Feb 28 23:03:47 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-

        user-name:"root" user-id:248  generated-at:2-28-2026T23:3:47
```

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）。