修复Catalyst SD-WAN安全建议 — 2026年2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：执行补救（TAC指导）

- 路径 A:未找到危害表现 — 升级
- 路径 B:确定的危害表现 — PSIRT指导

固定软件版本

附录：手动验证步骤（仅当无法进行管理技术收集时）

- 验证1:在身份验证日志中检查未授权的SSH登录
- 验证2:检查控制器系统日志中的未授权对等连接
- 验证3:DCA文件读取
- 验证4:路径遍历/任意文件覆盖
- 验证5:文件部署

常见问题解答

简介

本文档介绍根据2026年2月25日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漏洞
- Cisco Catalyst SD-WAN控制器身份验证旁路漏洞

这些PSIRT建议解决了以下缺陷：

- Cisco Bug ID CSCws52722
- Cisco Bug ID CSCws33583
- Cisco Bug ID CSCws33584
- Cisco Bug ID CSCws33585
- Cisco Bug ID CSCws33586
- Cisco Bug ID CSCws33587
- Cisco Bug ID CSCws93470

补救工作流程概述



注意：所有SD-WAN部署都存在漏洞，需要立即采取行动。但是，并非所有系统都显示危害迹象。

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
- 如果确定危害表现，则与PSIRT团队合作
- 如果未检测到危害表现，则提供升级指导和支持

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评估您的环境是否存在危害表现
4. 执行补救 — 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：在打开TAC案例之前，从所有控制组件收集管理技术文件。这对于TAC评估您的环境至关重要。

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：打开TAC案例并上传管理技术文件

收集第1步中的所有管理技术文件后，打开Cisco TAC支持案例。

所需操作：

1. 以适合您业务影响的严重性级别打开TAC案例
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. 参考PSIRT建议
4. 等待TAC评估和指导

⚠ 警告：TAC可确定您的系统状态，并建议适当的后续步骤。

没有技术支持中心(TAC)指导，请勿尝试进一步操作

步骤 3：TAC评估

TAC会分析上传的管理技术文件并确定您的系统状态。

在此期间：

- 请等待TAC进行正式评估，然后再采取任何措施
- TAC会联系您提供其调查结果和后续步骤

步骤 4：执行补救（TAC指导）

TAC会根据您的评估指导您完成适当的补救流程。完成TAC提供的所有说明。

路径 A:未找到危害表现 — 升级

如果TAC确认没有受到危害的迹象，请升级到固定软件版本。从本文档的固定软件版本表中选择适当的版本，并参考本部分中链接的升级指南。

⚠ 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

路径 B:确定的危害表现 — PSIRT指导

如果TAC确认存在危害表现，请完成TAC提供的所有指导。

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	20.9.8.2 *	20.9.8.2适用于vManage、vSmart和vBond的升级映像

应用于当前版本	固定版本	可用软件
20.10、20.11、20.12.5及更早版本	20.12.5.3	20.12.5.3 vManage、vSmart和vBond升级映像
20.12.6	20.12.6.1	20.12.6.1 vManage、vSmart和vBond升级映像
20.13、20.14、20.15.x	20.15.4.2	20.15.4.2 vManage、vSmart和vBond升级映像
20.16、20.17、20.18.x	20.18.2.1	20.18.2.1 vManage、vSmart和vBond升级映像

注意：对于CDCS(思科托管集群)上的客户，20.15.405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。

*如果您使用版本20.9或更早版本：您的版本(20.9.8.2)的固定软件于2027年2月提供。思科建议保留在当前主版本内并等待20.9.8.2版本，而不是升级到更高的主版本(20.12、20.15、20.18)。 如果您当前使用的版本低于20.9，请等待20.9.8.2升级。继续与TAC合作，并于2027年2月再次检查可用的软件链接。

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
```

然后运行以下命令：

```
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
```

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:DCA文件读取

步骤 1：查找内容

日志文件:/var/log/nms/containers/service-proxy/serviceproxy-access.log

日志行示例：

```
[2026-03-04T01:45:06.239Z] "GET /reports/data/opt/data/containers/config/data-collection-agent/.dca HTT

      " "python-requests/2.32.5" "ae076862-2244-45a6-844f-bc2af970e570" "192.168.2.3" "127.0.0.1:8080"
```

注意：IOC3不使用HTTP状态代码作为选通条件。记录任何遍历尝试。状态代码仍然与分析人员解释相关（例如，HTTP 200表示文件读取成功），但非200响应仍属于攻击尝试，必须进行评估。

步骤 2：手动搜索命令

从终端(Terminal) — 在解压的管理技术捆绑包中搜索：

```
zgrep -r "data-collection-agent/.dca" var/log/nms/containers/service-proxy/serviceproxy-access.log*
```

注意：合法DCA管理可以包括.dca URI（来自已知管理员IP地址）。升级之前，请务必根据已知管理员源验证源IP地址。将任一子类型的任何无法识别的源IP视为可疑。

验证4:路径遍历/任意文件覆盖

注意：IOC4仅适用于vManage设备。通过...../遍历写入文件的任何SmartLicensingManager日志条目都会标记，无论结果如何。如果日志中存在写入条目，则会发生写入。

步骤 1：查找内容

日志文件:/var/log/nms/vmanage-server.log

日志行示例：

```
06-Mar-2026 02:16:34,029 UTC INFO  [285fcdc0-30fa-4ca0-8e06-6953a095a59a] [LAB-TEST-1] [SmartLicensingM
04-Mar-2026 15:40:02,683 IST INFO  [ca0e641b-acc7-42a6-b39b-bf3d28be0bcb] [LAB-TEST-1] [SmartLicensingM
27-Feb-2026 08:49:27,169 IST INFO  [d9976a9d-071e-4e07-a3ef-4e90019cae12] [LAB-TEST-1] [SmartLicensingM
```

警告：示例中显示的文件名(例如cmd.gz.war)只是说明性文件。实际案例可以使用不同的文件名。记录标识的所有唯一遍历文件名，因为每个文件名代表单独的丢弃负载。

步骤 2：手动搜索命令

从终端(Terminal) — 在解压的管理技术捆绑包中搜索：

```
grep -rE "SmartLicensingManager.*Time taken to write file \.\.\/" var/log/nms/vmanage-server.log*
```

包括旋转/压缩日志：

```
zgrep -E "SmartLicensingManager.*Time taken to write file \.\.\/" var/log/nms/vmanage-server.log*
```

要捕获相关上下文行（上传API处理和写入事件），请执行以下操作：

```
grep -rE "SmartLicensingManager.*(write file|is processing|stringUrl|Failed to download).*/wildfly" var
```

验证5:文件部署

⚠ 警告：在受损环境中看到的文件扩展名可能有所不同。示例和搜索模式涵盖常见场景，但并非详尽无遗。

步骤 1：查找内容

日志文件:/var/log/nms/containers/service-proxy/serviceproxy-access.log

会标记对*.gz/*.jsp URI模式的任何POST请求。HTTP状态确定严重性：

HTTP状态	含义	确认危害受损？
200	服务器执行webshell;有效负载处于活动状态	是 — 确认的危害

日志行示例：

```
[2026-03-04T08:03:33.295Z] "POST /cmd.gz/cmd.jsp HTTP/1.1" 200 - 6 63 78 - "

      " "python-requests/2.32.5" "9d842c1a-b96f-4d04-ac3d-542ec3dd734b" "192.168.2.3" "127.0.0.1:8080"
```

步骤 2：手动搜索命令

从终端(Terminal) — 在解压的管理技术捆绑包中搜索：

```
grep -rE '"POST /[^"]+\.gz/[^"]+\.jsp HTTP' var/log/nms/containers/service-proxy/serviceproxy-access.lo
```

包括旋转/压缩日志：

```
zgrep -E '"POST /[^"]+\.gz/[^"]+\.jsp HTTP' var/log/nms/containers/service-proxy/serviceproxy-access.lo
```

要将已确认执行(HTTP 200)与非200次尝试分开，请执行以下操作：

```
# HTTP 200 only - confirmed webshell execution:
grep -rE '"POST /[^"]+\.gz/[^"]+\.jsp HTTP[^"]*" 200' var/log/nms/containers/service-proxy/serviceproxy
```

注意：记录所有唯一的源IP、总请求计数和HTTP 200响应计数。向思科TAC报告。

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，并打开TAC案例上传文件。TAC评估您的环境并提供后续步骤指导。

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: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：否，请等待TAC完成评估并提供指导，然后再尝试任何补救措施。

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:即将发布的20.15.5版本和其他即将发布的版本中是否包含PSIRT修复？

A：是，20.15.5和其他即将发布的版本中包含修复。但是，必须立即优先执行升级以缓解本文档中概述的漏洞。（不要等待！）

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：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CDCS/共享租户上。我们将升级到哪个版本？

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

1. Early Adopter clusters => 20.18.2.1（这实际上与标准版本相同）

2.建议版本集群=> 20.15.405（带PSIRT修复的CDCS特定版本）

CDCS客户无需采取任何有效措施来解决此PSIRT。

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
```

问:我们已经升级了，没有危害表现。在3月17日发布新的IOC后，我需要做什么？

A：列为固定版本的软件包含针对进一步尝试利用本文所介绍的两个建议中列出的CVE的防护。虽然升级可以防止将来发生漏洞，但可能存在现有漏洞，而这些漏洞在升级之前仍然存在。建议客户使用内置在Cisco Bug ID CSCws52722的Bug Search Tool页面上的自助服务“Check Bug Applicability”（检查Bug适用性），从控制组件重新扫描管理技术。如果需要，客户可以打开TAC案例并重复本文所述的过程，以根据新的IOC重新扫描管理技术。b

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）。