当SD-WAN Manager升级到20.15，而设备仍在运行17.12时，从CLI插件模板推送时，设备上缺少某些命令

目录

简介

本文档解释为什么在CLI附加模板中定义的某些命令行不再被推送到SD-WAN设备。从版本20.15开始，思科SD-WAN采用新的YANG模式。因此，当SD-WAN控制器升级到版本20.15时，但SD-WAN设备仍保留在较早的软件版本（例如17.12.x）上，某些CLI附加模板命令将不再传播到这些设备。

问题

您可能注意到，将SD-WAN控制器升级到版本20.15后，CLI附加模板中的某些命令不再出现，而设备仍保持版本17.12.x。设备升级到版本17.15后，问题也得到解决。

解决方案

有三种方法可以解决此问题：

1. 与不同CLI语句相关的几个缺陷可能导致此行为。其中一些缺陷提供了一些解决方法，可以在设备仍在运行旧软件版本时应用。如果受影响的CLI语句存在解决方法，请应用该解决方法，然后再次推送模板。

2. 使用功能模板而不是CLI附加模板。

3. 将设备升级到版本17.15。

缺陷	受影响的Cli	解决方法
CSCwj12763:漏洞搜索工具 CSCwh60190:漏洞搜索工具	ip name-server	ip name-server vrf <name> server-ip-list <list of servers IPs> ip name-server no-vrf <服务器列表>

CSCwm64335:漏洞搜索工具	IP 域名	已弃用IP域名
CSCwo92849:漏洞搜索工具	ip community-list	
CSCwm44407:漏洞搜索工具	route-map中的“description”和“match ip address” match ip address prefix-list xyz match ip address 33 描述集边缘路由社区	match ip address prefix-list-deprecated xyz match ip address access-list 33 description-DEPRECATED SET COMMUNITY FOR EDGE ROUTES
CSCwm07426:漏洞搜索工具	在路由映射中设置社区 ip community-list standard community1 permit internet set community internet additive set origin igp	ip community-list standard community1 permit-v1 permit-list internet set community-deprecated internet additive set origin-v1 igp
CSCwo69197:漏洞搜索工具	隧道模式IPSec IPv4	tunnel mode ipsec ipv4-old
CSCwj98144:漏洞搜索工具	ip host vbond.cisco.in 10.1.1.1	ip host vbond.cisco.in ip-list 10.1.1.1
CSCwj40573:漏洞搜索工具	允许ACL中的icmp any any echo 65 permit icmp any any echo	
CSCwo59694:漏洞搜索工具	aaa accounting network default start-stop group tacacs-10	
	aaa authentication enable default group tacacs-10 enable	aaa authentication enable default group-deprecated tacacs-20 enable-deprecated
CSCwn34168:漏洞搜索工具	track <tracker-name> endpoint-tracker	track tracked-object <tracker-name> endpoint-tracker

CSCwo95868:漏洞搜索工具	track 2 ip sla 2	track tracked-object 2 ip sla 2
CSCws30834:漏洞搜索工具	keepalive 3 5	keepalive-deprecated 3 5（正在等待修复）
CSCwn94547:漏洞搜索工具	选项67 ip 10.1.1.1	选项67 ip-deprecated 10.1.1.1
CSCws71815:漏洞搜索工具	在sd-wan路由器上更改“ip dhcp use class”命令的行为	ip dhcp use class"命令默认在17.15.x上启用，在17.12.x或更低版本上禁用
思科漏洞ID CSCwq57296:漏洞搜索工具	服务器专用	server-private-old

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）。