思科 ASA 系列 9.7(x) 版本说明

首次发布日期: 2017 年 01 月 23 日

上次修改日期: 2017 年 04 月 17 日

思科 ASA 系列 9.7(x) 版本说明

本文档包含有关思科 ASA 软件版本 9.7(x) 的版本信息。

重要说明

- 潜在的流量中断（9.7(1) 至 9.7(1.2)）— 漏洞 CSCvd78303 导致 ASA 可能会在运行 213 天后停止传输流量。这对于每个网络的影响是不同的，从连接受限问题，到停机等其他情况，可能都会涉及。您必须升级到没有此漏洞的新版本（新版本可用时）。同时，可以重新引导 ASA 以再获得 213 天的运行时间。可能还有其他解决方法。有关受影响的版本和详细信息，请参见现场通知 FN-64291。
- 在扩展/压缩环境中对 VPN IPv6 DTLS 进行 AnyConnect 远程访问可能会导致 ASA 流向回溯（例如：有大量隧道；或隧道与 ASA 头端器之间不断进行连接和断开连接）。**解决方法：**使用 IPv6 AnyConnect IKEv2 或 IPv4 AnyConnect DTLS VPN 远程访问会话类型。(CSCvc77123)
- ASA 9.x 中所用的 RSA 工具套件版本与 ASA 8.4 中所用的版本不同，这会导致两个版本之间的 PKI 行为出现差异。

  例如，运行 9.x 软件的 ASA 允许使用长度为 73 个字符的组织名称值 (OU) 字段导入证书。运行 8.4 软件的 ASA 允许您使用长度为 60 个字符的 OU 字段名称导入证书。由于存在此差异，因此可以在 ASA 9.x 中导入的证书无法导入到 ASA 8.4 中。如果尝试将 ASA 9.x 证书导入到运行 8.4 版的 ASA 中，可能会发生错误，“错误，导入 PKCS12 操作失败。

系统要求

本节列出了运行此版本需要满足的系统要求。

ASA 与 ASDM 兼容性

有关 ASA/ASDM 软件和硬件要求及兼容性信息（包括模块兼容性），请参阅 思科 ASA 兼容性。

VPN 兼容性

有关 VPN 兼容性，请参阅受支持的 VPN 平台和思科 ASA 5500 系列。

新增功能

本节列出了每个版本的新增功能。

注释 系统日志消息指南中列出了新增的、更改的和已弃用的系统日志消息。

ASA 9.7(1.4) 中的新增功能

发布日期：2017 年 4 月 4 日

注释 由于错误 CSCvd78303，已从 Cisco.com 删除了版本 9.7(1)。

功能	说明
平台功能	

功能	说明
使用集成路由和桥接的 ASA 5506-X 系列的新默认配置	ASA 5506-X 系列 将使用一种新默认配置。集成桥接和路由功能为使用外部第 2 层交换机提供了一种替代方法。对于替换 ASA 5505（其中包含硬件交换机）的用户，无需使用其他硬件即可借助此功能将 ASA 5505 替换为 ASA 5506-X 或其他 ASA 型号。 新默认配置包括： • 千兆以太网 1/1 上的外部接口、来自 DHCP 的 IP 地址 • 内部桥接组 BVI 1 及千兆以太网 ½（内部 1）至 1/8（内部 7）、IP 地址 192.168.1.1 • 内部 --> 外部流量 • 成员接口的内部 ---> 内部流量 • (ASA 5506W-X) 千兆以太网 1/9 上的 wifi 接口、IP 地址 192.168.10.1 • (ASA 5506W-X) WiFi <--> 内部，WiFi --> 外部流量 • 内部和 wifi 上的客户端的 DHCP接入点本身及其所有客户端均使用 ASA 作为 DHCP 服务器。 • 管理 1/1 接口启用，但未进行其他配置。ASA FirePOWER 模块随后可以使用此接口接入 ASA 内部网络，并将内部接口用作通向互联网的网关。 • ASDM 接入 - 允许内部和 wifi 主机。 • NAT - 从内部、wifi 和管理到外部的所有流量的接口 PAT。 如果您要升级，可以擦除您的配置然后使用 **configure factory-default** 命令应用默认配置，也可以手动配置 BVI 和桥接组成员以满足您的需求。请注意，为了便于允许桥接组内部通信，需要启用 **same-security-traffic permit inter-interface** 命令（此命令已存在于 ASA 5506W-X 默认配置中）。
ISA 3000 上的警报端口支持	ISA 3000 支持两个警报输入接口和一个警报输出接口。外部传感器（如门禁传感器）可以连接到警报输入。外部设备（如蜂鸣器）可以连接到警报输出接口。被触发的警报通过俩个 LED、系统日志、SNMP 陷阱以及连接到警报输出接口的设备传递。您可以配置外部警报的说明。您还可以为外部和内部警报指定严重性和触发条件。可对所有警报的中继、监控和日志记录进行配置。 我们引入了以下命令：**alarm contact description**、**alarm contact severity**、**alarm contact trigger**、**alarm facility input-alarm**、**alarm facility power-supply rps**、**alarm facility temperature**、**alarm facility temperature high**、**alarm facility temperature low**、**clear configure alarm**、**clear facility-alarm output**、**show alarm settings**、**show environment alarm-contact**。
ASAv10 上的 Microsoft Azure 安全中心支持	Microsoft Azure 是一个使用专用 Microsoft Hyper V 虚拟机监控程序的公共云环境。Microsoft Azure 安全中心是在 Azure 之上的 Microsoft 协调和管理层，可以简化高度安全的公共云基础设施的部署。将 ASAv 集成到 Azure 安全中心，这样您就可以将 ASAv 作为防火墙选项提供来保护 Azure 环境。

功能	说明

ISA 3000 的精确时间协议 (PTP)	ISA 3000 支持 PTP，它是用于某一网络中分布的各个节点的时间同步协议。由于该协议具有硬件时间戳功能，因此它可以提供比其他时间同步协议（如NTP）更高的精确度。ISA 3000 支持 PTP 转发模式，以及单步、端到端透明时钟。我们向默认配置添加了以下命令，以确保不会将 PTP 流量发送到 ASA FirePOWER 模块进行检查。如果您有现有部署，则需手动添加这些命令：
	
	`object-group service bypass_sfr_inspect`
	`  service-object udp destination range 319 320`
	`access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any`
	
	我们引入了以下命令： **debug ptp**、**ptp domain**、**ptp mode e2etransparent**、**ptp enable**、**show ptp clock**、**show ptp internal-info**、**show ptp port**

ISA 3000 的自动备份和自动恢复	可以使用 pre-set parameters in the backup 和 restore 命令中的预设参数来启用自动备份和/或自动恢复功能。这些功能的使用情形包括从外部介质的初始配置；设备更换；回滚到某一可操作状态。 我们引入了以下命令：**backup-package location**、**backup-package auto**、**show backup-package status**、**show backup-package summary**
防火墙功能	
支持 SCTP 多流重新排序、重组和分段。支持 SCTP 多宿主，其中 SCTP 终端具有一个以上的 IP 地址。	该系统现在完全支持 SCTP 多流重新排序、重组和分段，这样可以提高对 SCTP 流量的 Diameter 和 M3UA 检查的有效性。该系统还支持 SCTP 多宿主，其中每个 SCTP 终端都有一个以上的 IP 地址。对于多宿主，该系统可以打开辅助地址的针孔，使您无需编写访问规则即可允许它们访问。必须将每个 SCTP 终端限制为 3 个 IP 地址。 我们修改了以下命令的输出：**show sctp detail**。
改进了 M3UA 检查。	M3UA 检查现在支持状态化故障切换、半分布式集群和多宿主。您还可以配置严格应用服务器进程 (ASP) 状态验证和对各种消息的验证。严格 ASP 状态验证对于状态化故障切换和集群是必要的。 我们添加或修改了以下命令：**clear service-policy inspect m3ua session** [**assocID***id*]、**match port sctp**、**message-tag-validation**、**show service-policy inspect m3ua drop**、**show service-policy inspect m3ua endpoint**、**show service-policy inspect m3ua session**、**show service-policy inspect m3ua table**、**strict-asp-state**、**timeout session**。
支持 TLS 代理和思科 Unified Communications Manager 10.5.2 中的 TLSv1.2。	现在，您可以将包含 TLS 代理的 TLSv1.2 与思科 Unified Communications Manager 10.5.2 一起用于加密 SIP 或 SCCP 检查。TLS 代理支持作为 **client cipher-suite** 命令的组成部分添加的其他 TLSv1.2 密码套件。 我们修改了以下命令：**client cipher-suite**

功能	说明
集成路由和桥接	集成路由和桥接提供了在桥接组和路由接口之间路由的功能。桥接组是 ASA 进行桥接而非路由的接口组。ASA 并非真正的桥接，因为 ASA 仍将继续充当防火墙：将控制接口之间的访问控制，并将部署所有常见的防火墙检查。以前，您只能在透明防火墙模式下配置桥接组，而在这种模式下，您不能在桥接组之间进行路由。此功能使您可以在路由防火墙模式下配置桥接组，并在桥接组之间以及桥接组与路由接口之间进行路由。桥接组使用桥接虚拟接口 (BVI) 作为桥接组的网关参与路由。如果您在 ASA 上有额外的接口可以分配给桥接组，则集成路由和桥接提供了使用外部第2层交换机的替代方案。在路由模式下，BVI可以是指定接口，并且可以独立于成员接口单独参与某些功能，如访问规则和 DHCP 服务器。 以下功能在透明模式下受支持，但在路由模式下不受支持：多情景模式、ASA 集群。以下功能在 BVI 上也受支持：动态路由和组播路由。 我们修改了以下命令：**access-group**、**access-list ethertype**、**arp-inspection**、**dhcpd**、**mac-address-table static**、**mac-address-table aging-time**、**mac-learn**、**route**、**show arp-inspection**、**show bridge-group**、**show mac-address-table**、**show mac-learn**
VM 属性	您可以根据与 VMware vCenter 管理的 VMware ESXi 环境中的一个或多个虚拟机 (VM) 相关联的属性来定义网络对象，以筛选流量。您可以定义访问控制列表 (ACL)，以便将策略分配给来自共享一项或多项属性的 VM 组的流量。 我们添加了以下命令：**show attribute**。
用于内部网关协议的陈旧路由超时	现在您可以配置超时，用于删除内部网关协议（如 OSPF）的陈旧路由。 我们添加了以下命令：**timeout igp stale-route**。
路由功能	
31 位子网掩码	对于路由接口，您可以在 31 位子网上为点对点连接配置 IP 地址。31 位子网仅包含 2 个地址；通常，该子网中的第一个地址和最后一个地址保留用于网络和广播，因此无法使用 2 地址子网。不过，如果您有点对点连接，并且不需要网络或广播地址，则31位子网是保留 IPv4 中地址的一种有效方式。例如，2 个 ASA 之间的故障切换链接仅需 2 个地址；通过该链接的一端传输的任何数据包始终会被另一端接收，因此无需广播。您还可以拥有运行 SNMP 或系统日志的直连管理站。用于桥接组或组播路由的 BVI 不支持此功能。 我们修改了以屏幕：**ip address**、**http**、**logging host**、**snmp-server host**、**ssh**
高可用性和可扩展性功能	
FXOS 机箱上的 ASA 的站点间集群改进	现在，您可以在部署 ASA 集群时为每个 FXOS 机箱配置站点 ID。以前，您必须在 ASA 应用中配置站点 ID；此新功能简化了最初的部署。请注意，您不能再在 ASA 配置中设置站点 ID。此外，为了实现与站点间集群的最佳兼容性，我们建议您升级到 ASA 9.7(1) 和 FXOS 2.1.1，升级版包含对稳定性和性能的多项改进。 我们修改了以下命令：**site-id**

功能	说明
控制器本地化：对于数据中心的站点间集群改进	为了改善性能，并将流量保持在数据中心站点间集群的站点内，可以启用控制器本地化。新连接通常由指定站点内的集群成员进行负载均衡和拥有。不过，ASA 可为任何站点的成员分配控制器角色。控制器本地化可以启用其他控制器角色：与所有者在同一站点的本地控制器、和任何站点上的全局控制器。将所有者和控制器配置在同一站点可以改善性能。另外，如果原始所有者失败，则本地控制器将在同一站点选择一个新的连接所有者。如果集群成员收到由不同站点拥有的连接的数据包，则将使用全局控制器。 我们引入或修改了以下命令：**director-localization**、**show asp table cluster chash**、**show conn**、**show conn detail**
现在可以配置用于故障切换的接口链接状态监控轮询，以实现更迅速的检测	默认情况下，故障切换对中的每个 ASA 都会每隔 500 毫秒检查一次其接口的链接状态。现在，您可以在 300 毫秒与 799 毫秒之间配置轮训间隔；例如，如果您将轮训事件设置为 300 毫秒，则 ASA 就能更迅速地检测接口故障和触发故障切换。 我们引入了以下命令：**failover polltime link-state**
Firepower 9300 和 4100 上的主用/备用故障切换运行状况监控支持双向转发检测 (BFD)	您可以为 Firepower 9300 和 4100 上主用/备用对的两个单元之间的故障切换运行状况检查启用双向转发检测 (BFD)。将 BFD 用于运行状况检查比默认健康检查方法更可靠，并且 CPU 占用更少。 我们引入了以下命令：**failover health-check bfd**
VPN 功能	
用于 IKEv2 静态加密映射的动态 RRI	为 **crypto map** 指定 **dynamic** 时，将在成功建立 IPsec 安全关联 (SA) 后进行动态反向路由注入。根据商定的选择器信息添加路由。在删除 IPsec SA 后，这些路由会被删除。仅在基于静态加密映射的 IKEv2 上支持动态 RRI。 我们修改了以下命令：**crypto map set reverse-route**。
ASA VPN 模块支持虚拟隧道接口 (VTI)	使用名为虚拟隧道接口 (VTI) 的新逻辑接口对 ASA VPN 模块进行增强，该接口用于代表通向某一对等机的 VPN 隧道。这可通过将 IPsec 配置文件连接到隧道的每一端，为基于 VPN 的路由提供支持。使用 VTI 将不再需要配置静态加密映射访问列表并将其映射到接口。 我们引入了以下命令：**crypto ipsec profile**、**interface tunnel**、**responder-only**、**set ikev1 transform-set**、**set pfs**、**set security-association lifetime**、**tunnel destination**、**tunnel mode ipsec**、**tunnel protection ipsec profile**、**tunnel source interface**。
用于 AnyConnect 的基于 SAML 2.0 的 SSO	在专用网络中支持基于 SAML 2.0 的服务提供商 IdP。使用 ASA 作为用户与服务之间的网关，将通过限制匿名 webvpn 会话处理 IdP 上的身份验证，并将转换 IdP 与用户之间的所有流量。 我们添加了以下命令：**saml idp** 我们修改了以下命令：**debug webvpn saml**、**show saml metadata**

功能	说明
CMPv2	为了被定位为无线 LTE 网络中的安全网关设备，ASA 现在使用证书管理协议 (CMPv2) 支持某些管理功能。 我们修改了以下命令：**enrollment url**、**keypair**、**auto-update**、**crypto-ca-trustpoint**、**show crypto ca server certificates**、**show crypto key**、**show tech-support**
多重证书身份验证	现在，您可以使用 AnyConnect SSL 和 IKEv2 客户端协议验证每个会话的多重证书。已对聚合身份验证进行扩展，以定义多重证书身份验证的协议交换，并将此功能用于两种会话类型。 我们修改了以下命令：**authentication {[aaa] [certificate | multiple-certificate] | saml}**
提高分割隧道路由限值	AC-SSL 和 AC-IKEv2 的分割隧道路由限值已从 200 提高到了 1200。IKEv1 限值仍为 200。
Chrome 上的智能隧道支持	现已创建了一种新方法，用于 Mac 和 Windows 设备上的 Chrome 浏览器中的智能隧道支持。Chrome 智能隧道扩展已经替换了 Chrome 已不再支持的 Netscape 插件应用程序接口 (NPAPI)。如果您在没有安装该扩展的情况下点击了 Chrome 中启用了智能隧道的书签，则系统会将您重定向到 Chrome 网上应用店以获取该扩展。新的 Chrome 安装会将用户定向到 Chrome 网上应用店以下载该扩展。该扩展将从 ASA 下载运行智能隧道所需的二进制文件。除了安装新扩展的进程以外，您在使用智能隧道时的常用书签和应用配置将保持不变。
无客户端 SSL VPN：所有 Web 界面的会话信息	现在，所有 Web 界面都会显示当前会话的详情，包括用于登录的用户名，以及当前分配的用户权限。这让用户可以了解当前用户会话，还可提高用户的安全性。
无客户端 SSL VPN：Web 应用会话的所有 cookie 的验证	现在，所有 Web 应用都将仅在验证所有与安全相关的 cookie 后才会授予访问权限。在每次请求中，都会在向用户会话授予访问权限之前验证每个具有身份验证令牌或会话 ID 的 cookie。如果同一个请求中有多个会话 cookie，将导致该连接被丢弃。验证失败的 cookie 将被视为无效，并会将该事件添加到审核日志。
AnyConnect：现在，AnyConnect VPN 客户端连接的组策略中支持最大连接时间警告间隔。	警告间隔是达到最大连接时间之前的时间间隔，系统会向用户显示一条消息，提示他们连接将被终止。有效的时间间隔为 1-30 分钟。默认值为 30 分钟。以前无客户端和站点间 VPN 连接支持此功能。 现在，以下命令可以用于 AnyConnect 连接：**vpn-session-timeout alert-interval**
AAA 功能	
用于 AAA 的 LDAP 和 TACACS+ 服务器支持 IPv6 地址	现在，您可以将 IPv4 或 IPv6 地址用于 LDAP 和 TACACS+ 服务器（用于 AAA）。 我们修改了以下命令：**aaa-server host**、**test aaa-server**
管理功能	

功能	说明
对所有本地**用户名**和**启用**密码进行 PBKDF2 哈希处理	所有长度的本地**用户名**和**启用**密码都将使用 PBKDF2（基于密码的密钥派生功能 2）哈希值存储在配置中。以前，32 个字符或以下的密码使用基于 MD5 的哈希处理方法。已经存在的密码仍将继续使用基于 MD5 的哈希值，但您输入的新密码除外。有关降级指导原则，请参见《一般操作配置指南》中的“软件和配置”一章。 我们修改了以下命令：**enable password**、**username**
许可功能	
FXOS 机箱 上的故障切换对的许可变化	只有主用单元能够请求许可权利。以前，两个单元均可请求许可权利。支持 FXOS 2.1.1。
监控和故障排除功能	
traceroute 支持 IPv6 地址	**traceroute** 命令已修改为接受 IPv6 地址。 我们修改了以下命令：**traceroute**
支持用于桥接组成员接口的数据包跟踪器	现在，您可以将数据包跟踪器用于桥接组成员接口。 我们为 **packet-tracer** 命令添加了两个新选项：**vlan-id**和**dmac**
系统日志服务器支持 IPv6 地址	现在，您可以使用 IPv6 地址配置系统日志服务器，以记录和通过 TCP 和 UDP 发送系统日志。 我们修改了以下命令：**logging host**、**show running config**、**show logging**
SNMP OID 和 MIB	作为 ISA 3000 的精确时间协议 (PTP) 的组成部分，ASA 现在支持对应于端到端透明时钟模式的 SNMP MIB 对象支持以下 SNMP MIB 对象： • ciscoPtpMIBSystemInfo • cPtpClockDefaultDSTable • cPtpClockTransDefaultDSTable • cPtpClockPortTransDSTable

升级软件

本节提供了升级路径信息以及用来完成升级的链接。

升级路径

请参阅下表以获取您的版本的升级路径。某些版本需要先进行临时升级，然后才能升级到最新版本。

当前 ASA 版本	首先升级到：	然后升级到：
8.2(x) 及更早版本	8.4(6)	9.1(3) 及更高版本
8.3(x)	8.4(6)	9.1(3) 及更高版本
8.4(1) 至 8.4(4)	8.4(6) 或 9.0(2+)	9.1(3) 及更高版本
8.4(5+)	—	9.1(3) 及更高版本
8.5(1)	9.0(2+)	9.1(3) 及更高版本
8.6(1)	9.0(2+)	9.1(3) 及更高版本
9.0(1)	9.0(2+)	9.1(3) 及更高版本
9.0(2+)	—	9.1(3) 及更高版本
9.1(1)	9.1(2)	9.1(3) 及更高版本
9.1(2+)	—	9.1(3) 及更高版本
9.2(x)	-	9.2(2) 及更高版本
9.3(x)	-	9.3(2) 及更高版本
9.4(x)	-	9.4(2) 及更高版本
9.5(x)	—	9.5(2) 及更高版本
9.6(x)	—	9.6(2) 及更高版本
9.7(x)	—	9.8(1) 及更高版本

升级链接

要完成升级，请参阅升级到 ASA 9.7 和 ASDM 7.7。

尚未解决和已解决的漏洞

可通过思科缺陷搜索工具查看这一版本中尚未解决和已解决的缺陷。通过这一基于 Web 的工具，您可以访问思科缺陷追踪系统，其中记录了关于此本产品和其他思科硬件及软件产品的缺陷和漏洞信息。

注释 您必须拥有 Cisco.com 帐户才能登录并访问思科缺陷搜索工具。如果您还没有此帐户，请注册一个帐户。如果您没有思科支持合同，您只能通过 ID 查找缺陷，而无法使用搜索功能。

有关思科缺陷搜索工具的详细信息，请参阅缺陷搜索工具帮助及常见问题。

9.7(x) 版本中尚未解决的漏洞

如果您有思科支持合同，您可以使用以下动态搜索功能查找 9.7(x) 版本中严重程度在 3 级及以上的所有漏洞：

- 9.7 尚未解决的漏洞搜索

下表列出了在发布此版本说明时存在的尚未解决的漏洞。

警告 ID 号码	说明
CSCto19832	OpenLDAP 需要升级或修补
CSCva72318	XMLSoft libxml2 XML 内容处理外部实体扩展漏洞
CSCva72319	XMLSoft libxml2 格式字符串漏洞
CSCvc11628	预填充功能从错误的证书中（证书 1 设备）提取用户名，以获得双证书（与证书 2 用户相比）
CSCvc12313	cURL 和 libcurl Cookie 处理内容注入漏洞
CSCvc12314	cURL 和 libcurl 身份验证处理会话重用漏洞
CSCvc12315	cURL 和 libcurl 编码无界内存写入漏洞
CSCvc12316	cURL 和 libcurl curl_maprintf 功能内存双重释放漏洞
CSCvc12317	cURL 和 libcurl Kerberos 身份验证处理内存双重释放
CSCvc12318	cURL 和 libcurl 字符处理 URL 重定向漏洞
CSCvc31687	cURL 和 libcurl curl_getdate 功能无界内存读取漏洞
CSCvc31688	cURL 和 libcurl curl_easy_unescape 功能堆溢出漏洞
CSCvc31689	cURL 和 libcurl 共享 Cookie 处理“释放后使用”漏洞
CSCvc31690	Python smtplib StartTLS 居中管理漏洞
CSCvc53140	重新加载活动 ASA 后，OSPF 转播和 VPN 隧道丢失

警告 ID 号码	说明
CSCvc77123	使用 AnyConnect IPv6 DTLS 压缩方案时，ASA 可能会在 network_tcpmod_close_conn 中出现回溯

9.7(1.4) 版本中已解决的漏洞

下表列出了在发布此版本说明时已解决的选定漏洞。

警告 ID 号码	说明
CSCtw90511	数据包捕获导致多核平台上的 CPU 由于 spin_lock 而达到峰值
CSCuj69650	在“logging permit-hostdown”且 TCP 系统日志断开的情况下，ASA 仍会阻止新连接
CSCum70304	FIPS 自检开机故障 - fipsPostDrbgKat
CSCum74032	当 SNMP 轮询时，ASA 在备用设备上生成回溯
CSCup37416	过时的 VPN Context 条目导致 ASA 停止对流量加密
CSCup96099	“show resource usage detail counter all 1”导致 cpu 黑洞
CSCuq80704	ASA 错误地将 TCP 数据包分类为 PAWS 故障
CSCus37458	当处理组播数据包时，ASA 在线程名称 DATAPATH 中生成回溯
CSCut07712	ASA - TO the box 流量由于 asp 表路由中缺少 int. 而中断
CSCuu50708	ASA 在 9.1.5.19 上生成回溯
CSCuv86562	生成回溯：ASA 在线程名称 fover_health_monitoring_thread 的崩溃
CSCuw71147	在 http_header_by_name 中，Unicorn Proxy 线程中生成回溯
CSCuw95262	一段时间后闪存操作失败，且配置无法保存
CSCux08783	CWS：ASA 不附加 XSS 报头
CSCux08838	ASA：在 Checkheaps 中生成回溯
CSCux10499	智能隧道启动且 Java 关闭，无任何消息
CSCux11440	ASA 在 Unicorn Proxy Thread 中生成回溯

警告 ID 号码	说明
CSCux15273	show memory 指示的可用空闲内存不准确
CSCux17527	ASA 出现与僵尸网络相关的内存泄漏
CSCux18455	SNMP：内存泄漏遍历 CISCO-ENHANCED-MEMPOOL-MIB
CSCux29842	HA 中的主要和辅助 ASA 在线程名称：DataPath 中生成回溯
CSCux29929	ASA 9.4.2 在 DATAPATH 中生成回溯
CSCux35538	在具有 DHE 密码 SSL VPN scaled test 的 ctm_ssl_generate_key 中生成回溯
CSCux66866	流量由于 ASASM 上 arp 的恒定数量而下降
CSCux71197	“show resource usage”在 sh shut/no 后提供错误路由数
CSCux82835	当启用 asp transactional-commit nat 时，观察到 nat 池耗尽
CSCux86769	当连接回退至 TLS 时，VLAN 映射不起作用
CSCux92157	ASA 在具有组件 ssh 的线程名称：ssh_init 中生成回溯断言
CSCux94598	使用庞大动态 ACL 的 ASA 可能导致 Anyconnect 连接故障
CSCux95670	ASA 拒绝目标为 CX 的 to-the-box 流量
CSCux96716	将 Xlate 复制到备用/从站时，ASA 生成回溯
CSCux98029	ASA 重新加载，并在线程名称 DATAPATH 或 CP Processing 中生成回溯
CSCuy00215	更新 WR OS 至 RCPL 27
CSCuy00296	在线程：IPsec 报文处理程序中生成回溯
CSCuy01438	在启用了 SIP inspection 和 SFR 的情况下，ASA 9.5.2 会生成回溯
CSCuy05949	ASA：当发出 WRITE STANDBY 时主动情景中的 MAC 地址发生更改
CSCuy06125	重新添加情景即可创建情景，而无需在某些从站上配置情景
CSCuy07753	自 Firefox 32 位版本 43 起，智能隧道不工作
CSCuy11281	ASA：版本 9.4.2 中生成断言回溯

警告 ID 号码	说明
CSCuy15636	ASA 可能会在以下线程中生成回溯： DATAPATH-9-3101/DATAPATH-7-3145/DATAPATH-3-1685
CSCuy21206	当 diameter inspection 和 tls-proxy 导致丢包时，会生成回溯
CSCuy21287	在重新加载后，STBY ASA 不会通过 ASA-IC-6GE-SFP-B ifc 传递流量
CSCuy22561	VPN Load-Balancing 不发送 Ipv6 地址的负载均衡证书
CSCuy25163	思科 ASA ACL ICMP 回显请求代码过滤漏洞
CSCuy27428	升级至 9.1(7) 后 ASA 在线程名称 snmp 中生成回溯
CSCuy32321	在 ldap_client_thread 中生成回溯，并带有 ldap attr 映射和 pw mgmt
CSCuy32728	在配置了集群加密时，VPN LB 停止工作
CSCuy32964	在复制连接后，ASA 在集群成员或故障转移对的备用成员上崩溃
CSCuy34265	配置更改后，ASA 访问列表丢失并丢失元素
CSCuy36897	由于 ssl 错误无法导航至 OWA 2013
CSCuy39186	IKEv2 S2S 隧道由于先前的 sa 未删除而不出现
CSCuy40207	回溯：断言“0”失败：文件“ctm_daemon.c”
CSCuy41986	当链中的多个证书已验证时，OCSP 验证失败
CSCuy42223	BGP：配置失败，原因为仅在管理接口上受支持
CSCuy43839	当加密 L2L 数据包时，ASA 在线程名称：DATAPATH 中重新加载
CSCuy44472	BVI：接口 Ipv6 地址从 HA - A/A 上的备用情景删除
CSCuy45475	ASA：如果备用 IP 丢失，配置不会在配对上复制
CSCuy47706	Gtpv1_process_pdp_create_req 上生成回溯
CSCuy50406	Proxyi_rx_q_timeout_timer 中崩溃
CSCuy51918	RAMFS dirent 结构中的缓冲区溢出导致回溯
CSCuy54567	OpenSSL March 2016 的 pix-asa 评估

警告 ID 号码	说明
CSCuy55468	Unicorn Proxy Thread 导致 CP 争用
CSCuy57644	ASAv 子接口无法使用定制的 mac 地址发送流量
CSCuy60320	IPv6 Routes 未安装在 QP 上
CSCuy63642	处理出站 DTLS 数据包时 ASA 9.1(6) 生成回溯
CSCuy66942	思科 ASA 软件 DHCP Relay“拒绝服务”漏洞
CSCuy73652	在修改具有 FQDN 的对象组时，线程名称 idfw 中生成回溯
CSCuy74218	线程名称：DATAPATH 中生成与集群数据包重组有关的断言回溯
CSCuy78802	集群裂脑后，原主设备不会防御所有的 GARP 数据包
CSCuy80070	OSPF 路由不通过 L2L 隧道填充
CSCuy82905	全局访问列表配置被清除时，ASA 会崩溃
CSCuy85243	当收到具有不适当变量类型的 Radius 属性时，ASA 生成回溯
CSCuy87597	ASA - 在私钥解密期间 CP Processing 线程中生成回溯
CSCuy90936	ASA 可能停止响应 OSPF Hello 数据包
CSCuy92084	EC：FTP 辅助数据连接不会卸载
CSCuy95543	提高 malloc_avail_freemem() 的效率
CSCuz00077	ASA 9.1.6.4 在线程名称：telnet/ci 中生成回溯
CSCuz04534	当数据包冲击 PBR 和 WCCP 规则时，112 byte bin 中发生内存泄漏
CSCuz09255	在主动/主动 HA 中，ASA 不响应 NS
CSCuz09394	当在 var 后返回时，JS rewriter 状态机中发生无限循环
CSCuz10371	ASA 因 strncpy_sx.c 生成回溯和重新加载
CSCuz14600	重新加载后，Kenton 9.5.1“boot system/boot config”命令未保留
CSCuz14808	线程名称：idfw_proc 中生成 5585-10 回溯
CSCuz16398	NAT 转移表修改错误

警告 ID 号码	说明
CSCuz16498	控制台上显示错误消息“ERROR: Problem with interface”
CSCuz16565	9.6.2 EST - 断言“0”失败：文件“snp_vxlan.c”
CSCuz21068	CSCOPut_hash 会发起异常请求
CSCuz21178	线程名称 ssh 中生成 ASA 回溯
CSCuz22618	MH/MS：观察到生成回溯 - mh->mh_mem_pool < MEMPOOL_MAX_TYPE
CSCuz23354	当 GTP 中的计时器离队失败后，CPU 使用率高
CSCuz28000	如果集群中的所有设备重新加载，情景配置可能会被拒绝
CSCuz30425	带有名称的网络命令在重新加载后从 BGP 消失
CSCuz33255	IKEv2 Daemon 中生成回溯，并出现 20+ 秒 CPU 黑洞。
CSCuz34753	ASA QOS 无法在优先和最佳工作队列之间分类数据包
CSCuz36938	在编辑网络对象时，如果超出最大 snmp 主机数，即会生成回溯
CSCuz38115	当大型 ACL 应用到已启用对象组搜索的接口时，ASA 会生成回溯
CSCuz38180	ASA：启动后，备用 ASA 上的 DATAPATH 中生成 Page Fault 生成回溯
CSCuz38888	WebVPN 重写 MSCA Cert 注册页面/VBScript 失败
CSCuz40081	ASA 由于 vpnfo 发生内存泄漏
CSCuz40793	在 HA 配置同步期间，接口从 SFR 上删除
CSCuz42390	DRP 的 ASA 有状态故障切换间歇性地工作
CSCuz44687	当尝试获取自旋锁时，生成数据路径自死锁恐慌回溯
CSCuz44968	命令由于解析器开关而未安装在备用设备上
CSCuz52474	Pix-asa 的 Openssl 评估（2016 年 5 月）
CSCuz54193	ASA：在我们启用 SFR 流量重定向时，Datapath 中的 ASA 上生成回溯
CSCuz54545	生成 ASA Address not mapped 回溯 - 配置 snmp-server host
CSCuz61092	接口运行状况检查故障切换导致 OSPF 不将 ASA 作为 ABR 发布

警告 ID 号码	说明
CSCuz63531	调试 ospf 时观察到内存损坏、断言
CSCuz64603	处理数据时，在 gtp_update_sig_conn_timestamp 上生成 GTP 回溯
CSCuz64784	在情景删除期间，所有集群设备上的 DATAPATH 中生成 ASA 回溯
CSCuz66661	ASA Cut-through Proxy 不活动超时无效
CSCuz67349	ASA 集群碎片在传输之前未经检查而重组
CSCuz67590	ASA 可能在线程名称：cluster rx thread 中生成回溯
CSCuz67596	ASA 可能在线程名称：Unicorn Admin Handler 中生成回溯
CSCuz67690	由于存在无主设备升级的严重 Election 问题，ASA 崩溃
CSCuz68940	Crypto ca trustpool import 不会回落到数据路由表中
CSCuz70330	ASA：由于达到最大限制，SSH 在 ASA 设备上被拒绝
CSCuz72352	tls-proxy 握手期间生成回溯
CSCuz79013	当由于应用同步重新加载时，FTD 设备上的故障切换被禁用
CSCuz80281	Ipv6 邻居发现数据包处理行为
CSCuz90648	2048/1550/9344 字节块泄漏导致通信中断和模块故障
CSCuz92074	使用 PAT 的 ASA 未能转换不包含端口的 SIP Via 字段
CSCuz92921	ASA 在清除全局访问列表时崩溃
CSCuz94862	IKEv2：数据 rekey 冲突可能导致非活动 IPsec SA 卡住
CSCuz95806	DNS Doctoring DNS64 不工作
CSCuz98220	ASA 因线程名称：Dispatch Unit 生成回溯
CSCuz98704	升级后 CP Processing 线程中生成回溯
CSCva00190	由于芯片重置，ASA 9.4.2.6 中因 CTM 消息处理程序而 CPU 使用率高
CSCva00939	当解析了 FQDN 时，show access-lists 命令中显示 ACL 警告消息
CSCva01570	WebVPN 中 logon.html 文件存在意外的结尾

警告 ID 号码	说明
CSCva02817	ASA 没有速率限制，并且从服务器设置了 DSCP 位
CSCva03607	show service-policy output 报告错误值
CSCva03982	ASA：由于查找 PBR 而导致集群模式中的内存泄漏
CSCva10054	由于 sctp inspection，DATAPATH 中生成 ASA ASSERT 回溯
CSCva15911	重新加载 ASA 时，ASA 将 SSD 安装为磁盘 0，而不是闪存。
CSCva16471	当通过低度量路由时，IPv6 OSPF 路由不更新
CSCva22048	在多个通话中使用相同的媒体端口时，SIP 通话会因 PAT 断开
CSCva24924	当输入 config-url 时，9300 上的 ASA SM 通过 SSH 重新加载多情景
CSCva26771	ASA：PBR 因数据包丢包而发生内存泄漏
CSCva31378	在线程名称：rtcli async executor process 中生成 ASA 回溯
CSCva35439	ASA DATAPATH 回读（集群）
CSCva35990	具有 H323 inspection、rip h323_service_early_msg 的 CP Process 上生成回溯
CSCva36202	重新加载后，BGP 插槽在 ASA 上未打开
CSCva38556	思科 ASA 输入验证文件注入漏洞
CSCva39094	在进行 MPF 更改时，CLI 线程中生成 ASA 回溯
CSCva39804	在集群重新加入期间，接口从 SFR 上删除
CSCva40844	Crypto 加速器环超时导致丢包
CSCva43992	IKEv2 RA 证书身份验证。无法分配新的会话。达到最大会话数目
CSCva46920	当发出 show tls-proxy session detail 时，在线程名称：ssh 中生成回溯
CSCva47608	SCTP Mh：在具有双 nat 上的备用设备上，频繁删除和添加针孔
CSCva49256	ssh 中内存泄漏
CSCva62861	Uauth 在故障切换后失败
CSCva66278	SmartLic：机箱内主要切换许可证竞态条件

警告 ID 号码	说明
CSCva68987	禁用 ICMP 检查时，ASA 丢弃 ICMP 请求数据包
CSCva69584	OSPF 生成含错误掩码的 Type-5 LSA，在 LSDB 中卡住
CSCva69799	由于 FIPS 自检失败，ASA 卡在启动循环中
CSCva70095	当服务器处于 tls-proxy 中时，ASA 协商 TLS1.2
CSCva71783	响应回复数据包的 ICMP 错误数据被丢弃
CSCva76568	ASA：启用 IKEv1/IKEv2 会打开 RADIUS 端口
CSCva77852	ipsecvpn-ikev2_oth：5525 9.4.2.11 在线程名称：IKEv2 Daemon 中生成回溯
CSCva81749	当通过 IPSEC 协议连接时，未分配的 Ipv6 地址
CSCva84079	ASAv 经常在重新启动期间挂起
CSCva84635	ASA：CHILD_SA 冲突使 IKEv2 SA 断开
CSCva85382	CTS SGT 映射的 ASA 内存泄漏
CSCva85933	FTD - 6.1 - redistribute connected 将重新分配内部数据 (NLP)
CSCva87077	GTP 在回显响应的 gtpv1_process_msg 中生成回溯
CSCva87160	OTP 身份验证对无客户端 ssl vpn 无效
CSCva88796	AnyConnect 会话由于卡住的 L2TP Uauth 会话而无法连接
CSCva90806	当发出“show asp table classify domain permit”命令时，ASA 生成回溯
CSCva91420	CTM Message Handler 中生成 ASA 回溯
CSCva92151	思科 ASA SNMP 远程代码执行漏洞
CSCva92813	ASA 集群 DHCP Relay 不会将服务器响应发送至客户端
CSCva92975	ASA 5585-60 退出集群并生成回溯
CSCva94702	DP-CP 队列的排队故障可能会停止已检查的 TCP 连接
CSCva95686	FTD：9k 字节块消耗导致流量下降
CSCvb03994	IKE_DBG 中生成回溯

警告 ID 号码	说明
CSCvb05667	H.323 inspection 导致线程名称：CP Processing 中生成回溯
CSCvb05787	在应用 anyconnect 测试负载后，网络 udpmod_get 中生成回溯
CSCvb13737	wr mem/ wr standby 不在备用设备上同步配置
CSCvb14997	ASA DHCP Relay 重写作为 DHCP Offer 一部分收到的网络掩码和网关
CSCvb15265	线程名称：DATAPATH 中生成 ASA Page fault 回溯
CSCvb19251	ASA 作为 DHCP 中继丢弃 DHCP 150 Inform 消息
CSCvb19843	ASA 中的缓冲区溢出导致远程代码执行
CSCvb22435	线程名称 CP Processing 中由于 DCERPC inspection 生成 ASA 回溯
CSCvb22848	ASA 9.1.7-9 在线程名称：NIC status poll 中生成回溯
CSCvb27868	ASA 1550 块因多情景透明防火墙而消耗
CSCvb29411	如果仅可通过 mgmt vrf 访问，AAA 认证/授权失败
CSCvb29688	尽管已修复 CSCup37416，但过时的 VPN Context 条目仍会导致 ASA 停止对流量加密
CSCvb30445	当启用了“基于策略的路由”时，ASA 可能生成 DATAPATH 生成回溯
CSCvb31833	线程名称：DATAPATH-0-1790 中生成 ASA 回溯
CSCvb32297	WebVPN：VNC 插件：Java：对等机将连接重置：套接字写入错误
CSCvb32341	passive-interface default 导致 ASA 9.6(2) 上出现生成回溯
CSCvb36199	运行 9.6.2 的线程名称：snmp ASA5585-SSP-2 生成回溯
CSCvb39147	思科 ASA 平台上的 NFS 吞吐率降低
CSCvb43120	Checkheaps 线程中生成 ASA 回溯
CSCvb45039	线程名称 aaa_shim_thread 中生成 ASA 回溯
CSCvb47006	在自动更新线程上观察到 ASA 生成回溯。
CSCvb48640	Pix-asa 的 Openssl 评估（2016 年 9 月）

警告 ID 号码	说明
CSCvb49273	当来/往 ISE 发送/接收 CoA 时，CoA 会触发 ASA 上的生成回溯
CSCvb50301	ASA 在线程名称：rtcli 中生成回溯
CSCvb50750	FTD 在具有 sip 流量的故障切换期间崩溃
CSCvb52381	主站更换后，OSPF 会持续翻动
CSCvb52492	故障切换后，VPN 隧道由于 OSPF 路由问题而丢失
CSCvb52988	ASA 生成回溯线程名称：emweb/https
CSCvb55721	使用站点 ip 地址的多站点集群中的 ASA 完成 GARP flood
CSCvb58087	对象组搜索冗余服务对象被错误删除
CSCvb61056	9.6.2 TCP 连接不能通过 L2TP 工作
CSCvb63503	当由于时间范围被拒绝时，AAA 会话因 IKEv2 发生句柄泄漏
CSCvb63819	在升级操作系统 9.1.6 至 9.4.3 时，ASA-SM 因线程：fover_parse 生成回溯
CSCvb64161	ASA 很少重写客户端组播数据包的目标 MAC 地址
CSCvb68766	线程名称：IKE Daemon 中生成 ASA 回溯。
CSCvb74249	在多情景模式下配置了 TCP 系统日志的情况下，ASA 流量下降
CSCvb78614	4GE-SSM RJ45 接口可能会因接口“速率限制下降”而发生流量下降
CSCvb88126	ASA：尽管已修复 CSCuu48197，但卡住的 uauth 条目仍会拒绝 AnyConnect 连接
CSCvb92125	ASA 因在重写期间超出标签长度而丢弃 DNS PTR 应答
CSCvb92548	在启用了对象组搜索的情况下，ASA 匹配错误的 ACL
CSCvc00689	ASA：由于 ikev2 而发生内存泄漏
CSCvc05005	ASA 集群 TCP/SSL 端口在 LISTEN 状态上不显示
CSCvc07112	实现调度程序损坏问题的检测和自动修复功能
CSCvc07330	运行 webvpn 时，ASAv 可能会崩溃

警告 ID 号码	说明
CSCvc14190	在 EC 处于负载时，ASA 可能无法建立 SSL VPN 会话
CSCvc14448	9.6.2 - 在 AnyConnect IKEv2 性能测试期生成回溯
CSCvc14502	在不能到达 TCP 系统日志且设置了 logging permit-hostdown 的情况下，ASA 多情景不允许建立新连接
CSCvc19318	线程名称：sch_syslog 中生成 ASA 回溯
CSCvc23838	Webvpn CIFS 中发生思科 ASA 堆溢出
CSCvc24380	线程名称 IKE Daemon 上的 mqc_enable_qos_for_tunnel 处生成回溯
CSCvc24657	MIB 对象 cempMemPoolHCUsed 消失
CSCvc24788	ASA：OspfV3 路由不会安装
CSCvc25409	使用 SNMP 轮询时，CloneOctetString 中发生 ASA 内存泄漏
CSCvc33796	实施 ACL 和 NAT 表编译的速度改进
CSCvc36805	Firepower Threat Defense (FTD) IKEv2 NAT-T 在重新启动后禁用
CSCvc37557	SSL 连接在 ASA 和无客户端 WebVPN 的后端服务器之间挂起
CSCvc38425	带 FirePOWER 模块的 ASA 生成回溯并重新加载或导致进程未运行
CSCvc44240	ASA 集群：在 9.6.2 中，mac-address cmd 在跨端口通道接口上被忽略
CSCvc46502	FTD 集群 9K 块被碎片流量消耗
CSCvc48640	当配置了 forward-reference enable 时，ASA 未动态更新访问列表
CSCvc52072	对于登录到默认 webvpn 组的连接，Webvpn 门户网站未正确显示。
CSCvc52272	ASA 检查-MPF ACL 更改在 ASP 表上未正确排序
CSCvc52504	ASA 可能在线程名称：Unicorn Admin Handler 中生成回溯
CSCvc52879	重新加载主用/备用 ASA 故障切换对中的主用设备不会触发故障切换。
CSCvc55674	ASA：无法建立 IPSec SA
CSCvc55974	Ikev2 句柄在 L2L 设置中发生泄漏

警告 ID 号码	说明
CSCvc58272	ASA 错误地处理包装器中的负数，导致图形 webvpn 问题
CSCvc60254	SIP：含有多个段的 200 OK 消息重组错误
CSCvc62252	跟踪路由在无可达性时连接
CSCvc62556	ASA 集群线程名称：qos_metric_daemon 中生成回溯
CSCvc65409	在集群上的 gtpv2_process_msg 中观察到生成回溯
CSCvc68229	BGP 的 BFD 支持代码打开 tcp/udp 3784 和 3785 以绕过访问列表
CSCvc77123	使用 AnyConnect IPv6 DTLS 压缩方案时，ASA 可能会在 network_tcpmod_close_conn 中出现回溯
CSCvc79077	ASA watchdog 在启用了 rest-api 的 cluster config syn 期间生成回溯
CSCvc79371	未能对 ASA nat 池进行适当的更新。
CSCvc82146	线程名称 Datapath 中生成 ASA 回溯
CSCvc86554	生成回溯：主动设备上 ASA 9.5(2) 11 崩溃
CSCvc87914	ASA 因配置同步故障而生成回溯和重新加载
CSCvc88411	由于 Radius Accounting 数据包而出现 1550 字节块损耗
CSCvc92982	无法从 FMC 删除配置的自动 NAT
CSCvc93947	ASA(9.1.7.12)：通过备用 ASA 为组播流创建连接条目。
CSCvc96586	9K 块计数器发生问题，该问题会停止将流量弃踢到 snort，指示 snort 繁忙
CSCvc97734	当在端口通道接口上启用 management-only 时，部署失败
CSCvd01736	当使用 DHCP 时，L2TP 连接断断续续
CSCvd03261	重启后 ASAv 失去响应/VPN 无法工作
CSCvd08200	ASA 中缓慢内存泄漏
CSCvd14266	ASA 在 DATAPATH-41-16976 线程中生成回溯
CSCvd18126	ASA 在线程名称 DATAPATH 中生成回溯

警告 ID 号码	说明
CSCvd21541	在 ASA 944 中的服务对象组下创建端口对象后就无法删除
CSCvd21665	带 RRI 和 OSPF 的 ASA：无法从 ASP 路由表刷新路由
CSCvd23016	当使用 tftp 复制捕获输出时，ASA 可能会生成回溯
CSCvd23471	启动期间加载大型情景配置时，ASA 可能回生成回溯
CSCvd24066	当 IM 检查启用时，ASA 网络流量下降。
CSCvd28859	ASA：ICMP 流量的 PBR 内存泄漏
CSCvd33044	部署访问控制策略时，FTD 在“cli_xmlserver_thread”中崩溃
CSCvd33787	由于 uauth，syslog.c 中出现断言
CSCvd39113	尽管新设备未加入设置，但集群 C-Hash 表会再更新一台设备
CSCvd41052	9.6(2) 后计划程序队列损坏导致连接故障或故障切换问题
CSCvd41423	CRL 必须由包含 cRLSign 密钥使用的证书签署
CSCvd43309	新建对象组的访问列表不匹配
CSCvd47781	ASA 在执行服务中升级时生成回溯
CSCvd53884	模块重新加载后，Firepower (SFR) 模块数据面断开
CSCvd55983	在线程名称：dhcp_daemon 中生成回溯
CSCvd56292	默认的“global_policy”服务策略在重新启动后被删除
CSCvd62509	当 ASDM 显示“访问规则”时，ASA 在线程名称：accept/http 中生成回溯
CSCvd63718	ASA-FP9300 在线程名称 IPSEC MESSAGE HANDLER 中崩溃
CSCvd64416	ASA 所有情景在重新加载时使用相同的 EIGRP 路由器 ID
CSCvd64693	禁用和启用 EIGRP 后，EIGRP 路由错误地在 mgmt 路由表 vrf 上发布公告
CSCvd65797	将 NAT 相关对象更改为 fqdn 时，ASA 可能会崩溃
CSCvd69804	ASA - 接口状态更改导致使用 ipsec inner-routing-lookup 时 VPN 流量断开

警告 ID 号码	说明
CSCvd78303	在正常工作 213 天后，ARP 功能发生故障，因错误“punt-rate-limit-exceeded”而中断

最终用户许可协议

有关最终用户许可协议的信息，请访问 http://www.cisco.com/go/warranty。

相关文档

有关 ASA 的更多信息，请参阅思科 ASA 系列文档导航。