思科 ASA 系列 9.6(x) 版本说明

首次发布日期: 2016 年 03 月 21 日

上次修改日期: 2017 年 04 月 17 日

思科 ASA 系列 9.6(x) 版本说明

本文档包含有关思科 ASA 软件版本 9.6(x) 的版本信息。

重要说明

- 潜在的流量中断（9.6(2.1) 到 9.6(3)）- 由于漏洞 CSCvd78303，ASA 可能在正常运行 213 天后停止传输流量。对每个网络的影响是不同的，但是，从有限连接问题到停机等更加广泛的问题都可能出现。必须升级到不含此漏洞的新版本（如果可用）。同时，您可以重新启动 ASA 以获得额外 213 天的正常运行时间。可能还有其他解决方法。有关受影响的版本和更多信息，请参阅问题信息通告 FN-64291。
- ASAv 9.5.2(200) 功能（包括 Microsoft Azure 支持）在 9.6(1) 中不可用。 它们在 9.6(2) 中提供。
- ASDM 7.6(2) 在多情景模式下支持 AnyConnect 客户端配置文件。此功能需要 AnyConnect 4.2.00748 版或 4.3.03013 版及更高版本。
- (ASA 9.6.2) 使用多模式配置时的升级影响 - 从 9.5.2 升级到 9.6.1，然后升级到 9.6.2 时，多模式配置的任何现有 RAVPN 都将停止工作。在升级到 9.6.2 映像后，需要重新配置以便为每个情景提供存储空间并在所有情景中获得新的 AnyConnect 映像。
- (ASA 9.6(2)) 使用 SSH 公钥身份验证时的升级影响 - 由于对 SSH 身份验证的更新，需要其他配置来启用 SSH 公钥身份验证；因此，使用公钥身份验证的现有 SSH 配置在升级后不再有效。公钥身份验证默认用于 Amazon Web 服务 (AWS)，因此，AWS 用户将看到此问题。要避免丢失 SSH 连接，您可以在升级前更新您的配置。或者，您可以在升级后使用 ASDM（如果已启用 ASDM 访问）以修复该配置。

  用户名“admin”的原始配置示例：

  ```
  username admin nopassword privilege 15
  username admin attributes
    ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
    07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
  ```

  要使用 **ssh authentication** 命令，请在升级之前输入以下 命令：

  ```
  aaa authentication ssh console LOCAL
  ```

```
username admin password <password> privilege 15
```

我们建议 为该用户名设置密码，而不是保留 **nopassword** 关键字（如果存在）。 **nopassword** 关键字意味着可以输入 任何密码，而不是不可输入 任何 密码。在 9.6(2) 之前， **aaa** 命令 不是 SSH 公钥身份验证所需的，因此 **nopassword** 关键字未被触发。现在， **aaa** 命令 是必需的，它还会自动允许对 **username** 的常规密码身份验证，前提是 **password**（或 **nopassword**） 关键字存在。

在升级后，**username** 命令不再需要 **password** 或 **nopassword** 关键字；您可以要求用户不能输入密码。因此，要强制仅进行公钥身份验证，请重新输入 **username** 命令：

```
username admin privilege 15
```

- 在 Firepower 9300 上升级 ASA 时的升级影响 - 由于在后端进行的许可证授权命名更改，当升级到 ASA 9.6(1)/FXOS 1.1.4 时，启动配置可能在初始重新加载时无法正确解析；对应于追加授权的配置会被拒绝。

  对于独立 ASA，在设备重新加载新版本后，等待至所有授权得到处理并且处于“已授权”状态 (**show license all**)，只需再次重新加载 (**reload**) 而无需保存配置。在重新加载后，启动配置将被正确解析。

  对于故障切换对，如果您有任何追加授权，请按照 FXOS 版本说明中的升级程序进行操作，但在重新加载每台设备后需重置故障切换 (**failover reset**)。

  对于集群，请按照 FXOS 版本说明中的升级程序进行操作；无需进行其他操作。

- 升级至 9.5(x) 或更高版本时的 ASA 5508-X 和 5516-X 升级问题 - 在升级到 ASA 9.5(x) 或更高版本之前，如果您从未启用巨帧预留，则必须检查最大内存空间。由于制造缺陷，可能应用了错误的软件内存限制。如果在执行以下修复之前升级到 9.5 (x) 或更高版本，则您的设备将在启动时崩溃；在这种情况下，您必须使用 ROMMON 降级到 9.4（使用 ROMMON 加载 ASA 5500-X 系列的映像），执行下面的程序，然后再次升级。

  1. 输入以下命令以检查故障条件：

     ```
     ciscoasa# show memory detail | include Max memory footprint
     Max memory footprint        =    456384512
     Max memory footprint        =            0
     Max memory footprint        =    456384512
     ```

     如果对于“Max memory footprint”返回小于 **456,384,512** 的值，则表示存在故障条件，您必须在升级之前完成余下的步骤。如果显示的内存为 456,384,512 或更大值，则可以跳过此程序的剩余步骤，升级会正常进行。

  2. 进入全局配置模式：

     ```
     ciscoasa# configure terminal
     ciscoasa(config)#
     ```

  3. 暂时启用巨帧预留：

     ```
     ciscoasa(config)# jumbo-frame reservation
     WARNING: This command will take effect after the running-config
     is saved and the system has been rebooted. Command accepted.
     ```

```
INFO: Interface MTU should be increased to avoid fragmenting
jumbo frames during transmit
```

注释 不要重新加载 ASA。

4 保存配置：

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

5 禁用巨帧预留：

```
ciscoasa(config)# no jumbo-frame reservation
WARNING: This command will take effect after the running-config is saved and
the system has been rebooted. Command accepted.
```

注释 不要重新加载 ASA。

6 再次保存配置：

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

7 现在，您可以升级到 9.5(x) 或更高版本。

- 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 允许您使用长度为 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。由于此差异，可在 ASA 9.x 中导入的证书无法导入 ASA 8.4。如果尝试将 ASA 9.x 证书导入运行 8.4 版本的 ASA，则很可能会收到错误“ERROR: Import PKCS12 operation failed”。

系统要求

本部分列出了运行此版本的系统要求。

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。

新功能

本部分列出了每个版本的新功能。

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 9.6(3.1) 的新功能

发布日期：**2017** 年 **4** 月 **3** 日

注释 由于漏洞 CSCvd78303，已从 Cisco.com 中删除版本 Verion 9.6(3)。

特性	说明
AAA 功能	
对使用 SSH 公钥身份验证的用户以及使用密码的用户单独进行身份验证	在早于 9.6(2) 的版本中，您可以启用 SSH 公钥身份验证 (**ssh authentication**)，无需通过本地用户数据库 (**aaa authentication ssh console LOCAL**) 另外明确启用 AAA SSH 身份验证。在 9.6(2) 中，ASA 要求您明确启用 AAA SSH 身份验证。在此版本中，您不再必须明确启用 AAA SSH 身份验证；当您为用户配置 **ssh authentication** 命令时，默认情况下会为具有此类型身份验证的用户启用本地身份验证。此外，当您明确配置 AAA SSH 身份验证时，此配置仅适用于具有密码的用户名，而且您可以使用任何 AAA 服务器类型（例如 **aaa authentication ssh console radius_1**）。例如，某些用户可以利用使用本地数据库的公钥身份验证，而其他用户可以使用 RADIUS 密码。 未修改任何命令。

ASA 9.6(2) 的新功能

发布日期：**2016** 年 **8** 月 **24** 日

特性	说明
平台功能	

特性	说明
适用于 Firepower 4150 的 ASA	我们为 Firepower 4150 引入了 ASA。 需要 FXOS 2.0.1。 我们未添加或修改任何命令。
ASAv 上的热插接口	当系统处于活动状态时，您可以在 ASAv 上添加和删除 Virtio 虚拟接口。将新接口添加到 ASAv 时，虚拟机会检测并调配该接口。当您删除现有接口时，虚拟机会释放与该接口关联的所有资源。热插接口仅限于基于内核的虚拟机 (KVM) 虚拟机监控程序上的 Virtio 虚拟接口。
ASAv10 上提供 Microsoft Azure 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。ASAv 在 Hyper V 虚拟机监控程序的 Microsoft Azure 环境中充当访客。Microsoft Azure 上的 ASAv 支持一个实例类型，即标准 D3。标准 D3 可支持 4 个 vCPU、14 GB 内存和 4 个接口。 还在 *9.5(2.200)* 中。
ASAv 的管理 0/0 接口上的通过流量支持	现在，您可以允许 ASAv 上管理 0/0 接口的通过流量。过去，仅 Microsoft Azure 上的 ASAv 支持通过流量；现在所有 ASAvs 都支持通过流量。您可以选择将此接口配置为仅用于管理，但默认情况下，未此接口未配置。 我们修改了以下命令：**management-only**
通用标准认证	ASA 已更新，符合通用标准要求。请参阅下表中的各行，了解下列为 UCR 2013 认证添加的功能： • ASDM 的 ASA SSL 服务器模式匹配 • SSL 客户端 RFC 6125 支持： 安全系统日志服务器连接和智能许可连接的参考身份 ASA 客户端会检查服务器证书中的扩展密钥使用 当 ASA 作为 TLS1.1 和 1.2 的 TLS 客户端时进行相互身份验证 • PKI 调试消息 • 加密密钥归零验证 • 对 IKEv2 的 IPsec/ESP 传输模式支持 • 新系统日志消息
防火墙功能	
通过 TCP 的 DNS 检测	现在，您可以通过 TCP 流量 (TCP/53) 检测 DNS。 我们添加了以下命令：**tcp-inspection**

特性	说明
MTP3 用户适应性 (M3UA) 检测	现在，您可以检测 M3UA 流量，还可以根据点代码、服务指示器以及消息类和类型应用进行操作。 我们添加或修改了以下命令：**clear service-policy inspect m3ua** {**drops** | **endpoint** [*IP_address*]}、**inspect m3ua**、**match dpc**、**match opc**、**match service-indicator**、**policy-map type inspect m3ua**、**show asp table classify domain inspect-m3ua**、**show conn detail**、**show service-policy inspect m3ua** {**drops** | **endpoint***IP_address*}、**ss7 variant**、**timeout endpoint**
NAT 会话遍历实用程序 (STUN) 检测	现在，您可以检测 WebRTC 应用程序（包括 Cisco Spark）的 STUN 流量。检测会打开返回流量所需的针孔。 我们添加或修改了以下命令：**inspect stun**、**show conn detail**、**show service-policy inspect stun**
思科云 Web 安全的应用程序层运行状况检查	现在，您可以配置思科云 Web 安全，以在确定服务器是否正常时检查云 Web 安全应用程序的运行状况。通过检查应用程序运行状况，系统可以在主服务器响应 TCP 三向握手但无法处理请求时故障切换到备份服务器。这样可确保系统更可靠。 我们添加了以下命令：**health-check application url**、**health-check application timeout**
路由汇聚的连接抑制超时。	现在，您可以配置当连接使用的路由不再存在或处于非活动状态时，系统应保持连接的时间。如果路由在此抑制期间未变为活动状态，连接即会被释放。您可以减少抑制计时器，使路由汇聚更加快速地进行。但是，默认值 15 秒适合大多数网络，可以防止路由摆动。 我们添加了以下命令：**timeout conn-holddown** 还在 *9.4(3)* 中。
TCP 选项处理的变化	现在，在配置 TCP 映射时，您可以为数据包的 TCP 报头中的 TCP MSS 和 MD5 选项指定操作。此外，对 MSS、timestamp、window-size 和 selective-ack 选项的默认处理也已更改。以前使允许这些选项的，即使该报头中存在指定类型的多个选项也是如此。现在，默认情况下，如果数据包包含多个指定类型的选项，则会被丢弃。例如，以前允许有 2 个 timestamp 选项的数据包，而现在它会被丢弃。 您可以配置 TCP 映射，这样即可针对 MD5、MSS、selective-ack、timestamp 和 window-size 允许同一类型的多个选项。对于该 MD5 选项，以前的默认操作为清除该选项，而现在的默认操作是允许该选项。您还可以丢弃包含该 MD5 选项的数据包。对于 MSS 选项，您可以设置 TCP 映射中的最大报文段长度（按流量类）。所有其他 TCP 选项的默认操作均保持不变：被清除。 我们添加了以下命令：**tcp-options**
每个桥接组的透明模式最大接口数增加到 64	每个桥接组的最大接口数已从 4 增加到 64。 未修改任何命令。

特性	说明
透明模式下对组播连接的流量卸载支持。	现在，您可以卸载将在透明模式 Firepower 4100 和 9300 系列设备的网络接口卡中直接切换的组播连接。组播卸载仅适用于有且只有两个接口的桥接组。 此功能没有新的命令或 ASDM 屏幕。
可定制的 ARP 速率限制	您可以设置每秒允许的最大 ARP 数据包数。默认值取决于 ASA 型号。您可以自定义此值，以防止 ARP 风暴攻击。 我们添加了以下命令：**arp rate-limit**、**show arp rate-limit**
对于 IEEE 802.2 逻辑链路控制数据包的目标服务访问点地址的 Ethertype 规则支持。	现在，您可以为 IEEE 802.2 逻辑链路控制数据包的目标服务访问点地址编写 Ethertype 访问控制规则。由于此添加，**bpdu** 关键字不再匹配预期的流量。为 **dsap 0x42** 重写 **bpdu** 规则。 我们修改了以下命令：**access-list ethertype**
远程访问功能	
用于多情景模式的 Pre-fill/Username-from-cert 功能	AnyConnect SSL 支持得到扩展，允许在多情景模式下也可启用 pre-fill/username-from-certificate 功能 CLI，它们以前仅在单模式下可用。 未修改任何命令。
多情景模式下的 VPN 增强功能	多情景模式下的远程访问 VPN 现在支持闪存虚拟化。每个情景都留有专用存储空间和共享存储空间，具体根据可用的总闪存而定： • 专用存储 - 存储与该用户相关联的文件，并针对该用户所需的内容特定。 • 共享存储 - 启用后，可将文件上传到此空间，并使其可供任何用户情景进行读写访问。 未修改任何命令。
AnyConnect 客户端配置文件在多情景设备中受支持	AnyConnect 客户端配置文件在多情景设备中受支持。要使用 ASDM 添加新配置文件，您必须要有 AnyConnect 安全移动客户端版本 4.2.00748 或 4.3.03013 及更高版本。
漫游保护伞安全模块支持	没有 VPN 处于活动状态时，您可以选择配置 AnyConnect 安全移动客户端的漫游保护伞安全模块，以实现额外的 DNS 层安全保护。 未修改任何命令。
对 IKEv2 的 IPsec/ESP 传输模式支持	现在，ASA IKEv2 协商支持传输模式。它可以用于替代隧道（默认）模式。隧道模式封装整个 IP 数据包。传输模式只封装 IP 数据包的上层协议。传输模式要求源和目的主机都支持 IPSec，并且只有在隧道的目的对等体是 IP 数据包的最终目的时才可使用。 我们修改了以下命令：**crypto map set ikev2 mode**

特性	说明
针对 IPsec 内部数据包的按数据包路由查找	默认情况下，按数据包邻接查找针对外部 ESP 数据包执行；不对通过 IPsec 隧道发送的数据包执行查找。在某些网络拓扑中，如果路由更新修改了内部数据包的路径，但本地 IPsec 隧道仍正常运行，则通过该隧道的数据包可能无法正确路由，且无法到达其目的地。要避免此情况，请使用新选项为 IPsec 内部数据包启用按数据包路由查找。 我们添加了以下命令：**crypto ipsec inner-routing-lookup**
证书和安全连接功能	
ASA 客户端会检查服务器证书中的扩展密钥使用	系统日志和智能许可服务器证书必须在“Extended Key Usage”字段中包含“ServerAuth”。否则，连接会失败。
当 ASA 作为 TLS1.1 和 1.2 的 TLS 客户端时进行相互身份验证	如果服务器从 ASA 客户端请求客户端证书以进行身份验证，则 ASA 会发送为该接口配置的客户端身份证书。该证书由 **ssl trust-point** 命令配置。
PKI 调试消息	ASA PKI 模块会建立与 CA 服务器（例如 SCEP 注册、使用 HTTP 的撤销检查等）的连接。所有这些 ASA PKI 交换都会在调试加密 ca 消息 5 下记录为调试跟踪。
ASDM 的 ASA SSL 服务器模式匹配	对于通过证书进行身份验证的 ASDM 用户，您现在可以要求证书与证书映射匹配。 我们修改了以下命令：**http authentication-certificate match**
安全系统日志服务器连接和智能许可连接的参考身份	现在，TLS 客户端处理支持通过规则验证 RFC 6125 第 6 节中定义的服务器身份。仅在对系统日志服务器和智能许可服务器的 TLS 连接进行 PKI 验证时才会执行身份验证。如果所显示的身份无法根据配置的参考身份进行匹配，则表示未建立连接。 我们添加或修改了以下命令：**crypto ca reference-identity**、**logging host**、**call home profile destination address**
加密密钥归零验证	ASA 加密系统已更新，以符合新的密钥归零要求。必须将密钥全部覆盖为零，然后必须读取数据以确认写入是否成功。
SSH 公钥身份验证改进	在早期版本中，您可以启用 SSH 公钥身份验证 (**ssh authentication**)，无需通过本地用户数据库 (**aaa authentication ssh console LOCAL**) 另外启用 AAA SSH 身份验证。该配置现在已修复，因此您必须明确启用 AAA SSH 身份验证。要禁止用户使用密码而不是私钥，现在可以创建未定义任何密码的用户名。 我们修改了以下命令：**ssh authentication**、**username**
接口功能	
增加了 FXOS 机箱 上 ASA 的 MTU 大小	您可以在 Firepower 4100 和 9300 上将最大 MTU 设置为 9188 字节；以前，该最大值为 9000 字节。FXOS 2.0.1.68 及更高版本支持此 MTU。 我们修改了以下命令：**mtu**
路由功能	

特性	说明
双向转发检测 (BFD) 支持	ASA 现在支持 BFD 路由协议。添加对配置 BFD 模板、接口和映射的支持。还添加了对 BGP 路由协议使用 BFD 的支持。 我们添加或修改了以下命令：**authentication**、**bfd echo**、**bfd interval**、**bfd map**、**bfd slow-timers**、**bfd template**、**bfd-template**、**clear bfd counters**、**echo**、**debug bfd**、**neighbor fall-over bfd**、**show bfd drops**、**show bfd map**、**show bfd neighbors**、**show bfd summary**
IPv6 DHCP	ASA 现在支持 IPv6 寻址的以下功能： • DHCPv6 地址客户端 - ASA 从 DHCPv6 服务器获取 IPv6 全局地址和可选的默认路由。 • DHCPv6 前缀授权客户端 - ASA 从 DHCPv6 服务器获取授权的前缀。然后，ASA 可以使用这些前缀来配置其他 ASA 接口地址，以便无状态地址自动配置 (SLAAC) 客户端可以自动配置同一网络上的 IPv6 地址。 • 授权前缀的 BGP 路由器通告 • DHCPv6 无状态服务器 - SLAAC 客户端向 ASA 发送信息请求 (IR) 数据包时，ASA 会提供其他信息，例如域名。ASA 仅接受 IR 数据包，并且不会为客户端分配地址。 我们添加或修改了以下命令：**clear ipv6 dhcp statistics**、**domain-name**、**dns-server**、**import**、**ipv6 address autoconfig**、**ipv6 address dhcp**、**ipv6 dhcp client pd**、**ipv6 dhcp client pd hint**、**ipv6 dhcp pool**、**ipv6 dhcp server**、**network**、**nis address**、**nis domain-name**、**nisp address**、**nisp domain-name**、**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix**、**sip address**、**sip domain-name**、**sntp address**
高可用性和可扩展性功能	
缩短了在使用主用/备用故障切换时从 AnyConnect 同步动态 ACL 的时间	如果您在故障切换对上使用 AnyConnect，将关联的动态 ACL (dACL) 同步到备用设备的时间现在已缩短。以前使用大型 dACL 时，同步时间可能会花费数小时，在此期间备用设备会忙于同步而不是忙于提供高性能的备份。 未修改任何命令。
许可功能	

特性	说明
ASAv 永久许可证保留	在不允许与 Cisco Smart Software Manager 之间进行通信的高安全性环境中，您可以请求 ASAv 永久许可证。在 9.6(2) 中，我们还为 Amazon Web 服务上的 ASAv 添加了对此功能的支持。Microsoft Azure 不支持此功能。 **注释** 并非所有帐户都被批准使用永久许可证预留。在您尝试配置此功能之前，请确保已获得思科批准。 我们引入了以下命令：**license smart reservation**、**license smart reservation cancel**、**license smart reservation install**、**license smart reservation request universal**、**license smart reservation return** 还在 *9.5(2.200)* 中。
ASAv短字符串永久许可证预留增强功能	由于对智能代理进行了更新（更新到1.6.4），请求和授权码现在使用更短的字符串。 未修改任何命令。
FXOS 机箱 上 ASA 的永久许可证预留	在不允许与 Cisco Smart Software Manager 之间进行通信的高安全性环境中，您可以在 Firepower 9300 和 Firepower 4100 上请求 ASAv 永久许可证。所有可用许可证授权都包含在永久许可证中，包括标准层、强加密（如果符合条件）、安全情景和运营商许可证。需要 FXOS 2.0.1。 所有配置均在 FXOS 机箱 上执行；在 ASA 上无需配置。
ASAv 到 v1.6 的智能代理升级	智能代理从 1.1 版本升级到 1.6 版本。此升级支持永久许可证保留，同时也支持依据许可证账号中的权限集设置强加密 (3DES/AES) 许可证授权。 **注释** 如果您从 9.5(2.200) 版本降级，ASAv 将不保留许可注册状态。您需要使用 **license smart register idtoken***id_token***force** 命令重新注册；从 Smart Software Manager 中获取 ID 令牌。 我们引入了以下命令：**show license status**、**show license summary**、**show license udi**、**show license usage** 我们修改了以下命令：**show license all**、**show tech-support license** 我们弃用了以下命令：**show license cert**、**show license entitlement**、**show license pool**、**show license registration** 还在 *9.5(2.200)* 中。
监控功能	
类型为 asp drop 的数据包捕获支持 ACL 和匹配过滤	当您创建类型为 asp-drop 的数据包捕获时，现在还可以通过指定 ACL 或匹配选项来限制捕获范围。 我们修改了以下命令：**capture type asp-drop**

特性	说明
调查分析增强功能	您可以创建在 ASA 上运行的任何进程的核心转储。ASA 还会提取您可从 ASA 复制的主要 ASA 进程的文本部分，以便进行检查。 我们修改了以下命令：**copy system:text**、**verify system:text**、**crashinfo force dump process**
通过 NetFlow 按连接跟踪数据包计数	添加了两个计数器，以允许 Netflow 用户查看在连接的两个方向上正在发送的第 4 层数据包数。您可以用这些计数器来确定平均数据包速率和大小，更好地预测流量类型、异常和事件。 未修改任何命令。
用于故障切换的 SNMP engineID 同步	在故障切换对中，已配对 ASA 的 SNMP engineID 会在两个设备上同步。每个 ASA 都保存了 3 组 engineID：同步 engineID、本地 engineID 和远程 engineID。 SNMPv3 用户也可在创建配置文件以保留本地化 **snmp-server user** 身份验证和隐私选项时指定 ASA 的 engineID。如果用户不指定本地 engineID，**show running-config** 输出将显示每位用户的 2 个 engineID。 我们修改了以下命令：**snmp-server user** 还在 *9.4(3)* 中。

ASA 9.6(1) 的新功能

发布日期：2016 年 3 月 21 日

注释 ASAv 9.5.2(200) 功能（包括 Microsoft Azure 支持）在 9.6(1) 中不可用。它们在 9.6(2) 中提供。

特性	说明
平台功能	
适用于 Firepower 4100 系列 的 ASA	我们为 Firepower 4110、4120 和 4140 引入了 ASA。 需要 FXOS 1.1.4。 我们未添加或修改任何命令。
针对 ISA 3000 的 SD 卡支持	现在，您可以将 SD 卡用作 ISA 3000 的外部存储。该卡在 ASA 文件系统中显示为 disk3。请注意，即插即用支持需要硬件版本 2.1 及更高版本。使用 **show module** 命令检查您的硬件版本。 我们未添加或修改任何命令。

特性	说明
对 ISA 3000 的双电源支持	对于 ISA 3000 中的双电源，您可以建立双电源作为 ASA 操作系统中的预期配置。如果一个电源出现故障，ASA 会发出警报。默认情况下，ASA 需要单个电源，只要包含一个正常工作的电源就不会发出警报。 我们引入了以下命令：**power-supply dual**。
防火墙功能	
直径检测改进	您可以通过 TCP/TLS 流量检测直径，应用严格的协议符合性检查，并在集群模式下通过 SCTP 检测直径。 我们引入或修改了以下命令：**client clear-text**、**inspect diameter**、**strict-diameter**。
集群模式下的 SCTP 有状态检测	现在，SCTP 有状态检测可在集群模式下工作。您还可以在集群模式下配置 SCTP 全状态检测绕行。 我们未添加或修改任何命令。
支持对在 H.225 SETUP 消息发送到之前到来的 H.255 FACILITY 消息进行 H.323 检测以实现 H.460.18 兼容性。	现在，您可以配置 H.323 检测策略映射以允许 H.225 FACILITY 消息在 H.225 SETUP 消息发送到之前到来，当终端符合 H.460.18 时会出现这种情况。 我们引入了以下命令：**early-message**。
对安全交换协议 (SXP) 版本 3 的思科 Trustsec 支持。	ASA 上的思科 Trustsec 现在实施 SXPv3，从而支持 SGT 到子网绑定，实现比主机绑定更高的效率。 我们引入或修改了以下命令：**cts sxp mapping network-map***maximum_hosts*、**cts role-based sgt-map**、**show cts sgt-map**、**show cts sxp sgt-map**、**show asp table cts sgt-map**。
对 Firepower 4100 系列 的流量卸载支持。	您可以识别需从 ASA 中卸载并直接在 Firepower 4100 系列 的 NIC 中切换的流量。 需要 FXOS 1.1.4。 我们未添加或修改任何命令。
远程访问功能	
IKEv2 分段，RFC-7383 支持	ASA 现在支持 IKEv2 数据包的此标准分段。这允许与其他 IKEv2 实施（例如 Apple、Strongswan 等）的互操作性。ASA 会继续支持当前的专有 IKEv2 分段，以保持与不支持 RFC-7383 的思科产品（例如 AnyConnect 客户端）的向后兼容性。 我们引入了以下命令：**crypto ikev2 fragmentation**、**show running-config crypto ikev2**、**show crypto ikev2 sa detail**
Firepower 9300 和 Firepower 4100 系列上的 VPN 吞吐量性能增强功能	现在，Firepower 9300 和 Firepower 4100 系列 上的 ASA 安全模块支持 **crypto engine accelerator-bias** 命令。此命令让您可以将更多加密核心“偏移”到 IPSec 或 SSL。 我们修改了以下命令：**crypto engine accelerator-bias**

特性	说明
可配置的 SSH 加密和 HMAC 算法。	用户可以在执行 SSH 加密管理时选择密码模式，并且可以为不同的密钥交换算法配置HMAC和加密。您可能需要将密码更改为更强或更弱，具体取决于您的应用程序。请注意，安全复制的性能部分取决于使用的加密密码。默认情况下，ASA 按顺序协商以下其中一种算法：3des-cbc、aes128-cbc、aes192-cbc、aes256-cbc、aes128-ctr、aes192-ctr、aes256-ctr。如果选择建议的第一个算法 (3des-cbc)，则性能比更高效的算法（如 aes128-cbc）要慢得多。例如，要更改建议的密码，可使用 **ssh cipher encryption custom aes128-cbc**。 我们引入了以下命令：**ssh cipher encryption**、**ssh cipher integrity**。 同样适用于 *9.1(7)*、*9.4(3)* 和 *9.5(3)* 版本。
对 IPv6 的 HTTP 重新定向支持	为 ASDM 访问或无客户端 SSL VPN 启用 HTTP 重新定向到 HTTPS 时，现在可以将发送的流量重新定向到 IPv6 地址。 我们为以下命令添加了功能：**http redirect** 同样适用于 *9.1(7)* 和 *9.4(3)* 版本。
路由功能	
IS-IS 路由	ASA 现在支持中间系统到中间系统 (IS-IS) 路由协议。系统添加了以下支持：可以使用 IS-IS 协议路由数据、执行身份验证以及重新分发和监控路由信息。 我们引入了以下命令：**advertise passive-only**、**area-password**、**authentication key**、**authentication mode**、**authentication send-only**、**clear isis**、**debug isis**、**distance**、**domain-password**、**fast-flood**、**hello padding**、**hostname dynamic**、**ignore-lsp-errors**、**isis adjacency-filter**、**isis advertise prefix**、**isis authentication key**、**isis authentication mode**、**isis authentication send-only**、**isis circuit-type**、**isis csnp-interval**、**isis hello-interval**、**isis hello-multiplier**、**isis hello padding**、**isis lsp-interval**、**isis metric**、**isis password**、**isis priority**、**isis protocol shutdown**、**isis retransmit-interval**、**isis retransmit-throttle-interval**、**isis tag**、**is-type**、**log-adjacency-changes**、**lsp-full suppress**、**lsp-gen-interval**、**lsp-refresh-interval**、**max-area-addresses**、**max-lsp-lifetime**、**maximum-paths**、**metric**、**metric-style**、**net**、**passive-interface**、**prc-interval**、**protocol shutdown**、**redistribute isis**、**route priority high**、**route isis**、**set-attached-bit**、**set-overload-bit**、**show clns**、**show isis**、**show router isis**、**spf-interval**、**summary-address**。
高可用性和可扩展性功能	
在路由、跨网络的 EtherChannel 模式下对站点特定的 IP 地址的支持	对于跨网络 EtherChannel 的路由模式下的站点间集群，现在除了站点特定的 MAC 地址外还可以配置站点特定IP地址。添加站点IP地址使您可以在重叠传输虚拟化 (OTV) 设备上使用 ARP 检测，以防止来自全局 MAC 地址的 ARP 响应通过数据中心互联 (DCI) 传输，否则会导致路由问题。对于无法使用 VACL 来过滤 MAC 地址的某些交换机，需要 ARP 检测。 我们修改了以下命令：**mac-address**、**show interface**

特性	说明
管理功能	
对本地 **用户名** 和 **启用** 密码的更长密码支持（多达 127 个字符）	现在，您可以创建长度多达 127 个字符（以前的限制为 32）的本地 **username** 和 **enable** 密码。在创建长度超过 32 个字符的密码时，密码存储在使用 PBKDF2（基于密码的密钥派生函数 2）散列的配置中。较短的密码会继续使用基于 MD5 的散列方法。 我们修改了以下命令：**enable**、**username**。
CISCO-ENHANCED-MEMPOOL-MIB 中对 cempMemPoolTable 的支持	现在，支持 CISCO-ENHANCED-MEMPOOL-MIB 的 cempMemPoolTable。这是一个内存池表，用于监控托管系统中所有物理实体的条目。 **注释** CISCO-ENHANCED-MEMPOOL-MIB 使用 64 位计数器，并且支持在具有超过 4GB RAM 的平台上报告内存。 我们未添加或修改任何命令。 同样适用于 *9.1(7)* 和 *9.4(3)* 版本。
REST API 1.3.1 版本	我们增加了对 REST API 1.3.1 版本的支持。

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

当前 ASA 版本	首先升级到：	然后升级到：
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 9.6 和 ASDM 7.6。

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 查找漏洞，而无法使用搜索功能。

有关思科漏洞搜索工具的详细信息，请参阅漏洞搜索工具帮助及常见问题。

9.6(x) 版本中尚未解决的漏洞

下表列出了在发布此版本说明时尚未解决的漏洞。

Caveat ID 号码	说明
CSCvb21927	第三方 IKEv2 证书身份验证 PRF SHA2 互操作性
CSCvb97470	asa Rest-api - 组件监控 - 空值/空白值

Caveat ID 号码	说明
CSCvb98012	设置不是以 VPN 为目标的逆向路由黑洞流量
CSCvc07112	调度程序损坏会导致双主用故障切换和/或控制台无响应
CSCvc31902	在密钥重新生成期间丢包，且 PPS 较高
CSCvc54069	Firepower 威胁防御默认 VPN 路由在重新加载后损坏
CSCvc56526	CEP 记录编辑页面加载需要数分钟
CSCvc56919	通过 IPv4 隧道发送的逆向 UDP/TCP IPv6 流量出现流量丢失
CSCvc61322	ASA“inspect ipsec-pass-thru”导致通过 VPN 进行单向连接
CSCvc62492	ASA：文件系统在正常运行很长时间后变为只读
CSCvc85369	ASA 不响应 IPv6 MLD 查询。
CSCvc88329	FTD - 定义目标区域后，访问控制策略与组播流量不匹配
CSCvc88607	备用 ASA 从主用 ASA 接收的 OSPF 路由未安装在 RIB 上
CSCvd01130	当 IP 电话在 VPN 隧道后时，ASA TCP SIP 检测转换不起作用
CSCvd01218	ASA IPv6 邻居转到 INCMP（不完整），然后得到恢复
CSCvd15843	当传递数据时，端口转发会话由于组策略中的“vpn-idle-timeout”而超时
CSCvd19162	在用户情景中发出写备用时，备用 ASA 进入故障状态
CSCvd25094	修改接口时出现回溯。interface_action.c 中出现断言
CSCvd26699	ASA 错误地触发系统日志 ID 201011
CSCvd28852	ASA 界面配置丢失 nameif
CSCvd29265	配置接口区域时出现回溯
CSCvd33348	在尝试生成 EIGRP 错误信息系统日志时出现回溯
CSCvd36411	配置为 TD 回避例外的主机被回避
CSCvd42723	服务策略集连接中出现负连接计数器
CSCvd47111	calendar_queue.h 中出现断言回溯，线程名称：DATAPATH

Caveat ID 号码	说明
CSCvd47146	在启用 object-group-search 的情况下，大型 ACL 更改期间出现回溯
CSCvd47298	线程名称“PIM IPv4”中出现回溯
CSCvd49262	尝试保存/查看具有巨型对象组 (display_hole_og) 的访问列表时出现回溯
CSCvd49270	线程名称为 DATAPATH 的 5 元组查找中出现回溯
CSCvd49550	当 managment0/0 用作 src-ip 时，9.5.1 及更高版本的 ASA 不显示 SXP 套接字
CSCvd51826	核心处理控制点繁忙时，一些命令导致管理会话中断。
CSCvd53381	当由于时间范围 ACL 而保存/查看配置时出现 ASA 回溯
CSCvd53401	当清除 eigrp 配置时看到回溯
CSCvd58094	已配置 PBR 时，ARP 线程中出现 ASA 回溯
CSCvd64416	在重新加载时，ASA 所有情景使用同一 EIGRP 路由器 ID
CSCvd64693	禁用再启用 EIGRP 后，在管理路由表 vrf 中错误地发布 EIGRP 路由
CSCvd66414	在 ASA 故障切换对中显示连接计数不匹配
CSCvd67907	ASA SSL 客户端不响应重新协商请求
CSCvd68137	将 ASA 从 9.5 升级到 9.6.2 后，无法通过 Rest API 读取合规性状态
CSCvd68437	在重新加载备用设备且有数以百计包含无法解决的 FQDN 的 ACL 时，故障切换会受阻
CSCvd68518	线程名称 Unicorn Admin Handler 中出现回溯
CSCvd69804	ASA - 在使用 ipsec inner-routing-lookup 时，接口状态更改导致 VPN 流量断开
CSCvd71473	ASA：当使用许多 DNS 查询时出现缓慢的内存泄漏
CSCvd73468	由于空闲超时，集群目录连接超时
CSCvd74140	ASAv 在从 9.6.1 升级到 9.6.2 后丢失许可证注册
CSCvd76821	tcp-options md5 allow 作为 tcp-options md5 clear 推送到从属设备
CSCvd76939	ASA 策略映射配置未复制到从属集群

已修复的漏洞

本部分列出了每个版本的已解决问题。

9.6(3.1) 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
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
CSCum28756	ASA：设备重新加入集群后，对 SNMPv3 轮询的身份验证失败
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
CSCuq80704	ASA 错误地将 TCP 数据包分类为 PAWS 故障
CSCus29600	dhcprelay 接口不随着路由的更改而出现更改
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
CSCuv61791	ASA 上的 CWS 重新定向可能损坏 https 流量的序列号
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
CSCuw88759	ASA：协议和状态显示 UP 但未连接接口
CSCuw95262	一段时间后闪存操作失败，且配置无法保存
CSCux17527	ASA 出现与僵尸网络相关的内存泄漏
CSCux92157	ASA 在具有组件 ssh 的线程名称：ssh_init 中生成回溯断言
CSCux98029	ASA 重新加载，并在线程名称 DATAPATH 或 CP Processing 中生成回溯
CSCuy22155	ASA 生成意外系统日志消息，且组播路由已禁用
CSCuy43438	与客户端断开连接后，无法通过 IPSec 连接 L2TP。

警告 ID 号码	说明
CSCuy47545	重新加载 stdby 916.9 或更高版本后，多情景中缺少 http 配置
CSCuy55468	Unicorn Proxy Thread 导致 CP 争用
CSCuy89288	AnyConnect DTLS 按需 DPD 未间歇性地发送
CSCuz09255	在主动/主动 HA 中，ASA 不响应 NS
CSCuz42390	DRP 的 ASA 有状态故障切换间歇性地工作
CSCuz44968	命令由于解析器开关而未安装在备用设备上
CSCuz64603	处理数据时，在 gtp_update_sig_conn_timestamp 上生成 GTP 回溯
CSCuz72244	错误指示和空 TID MBReq 丢弃，没有 Ctrl F-TEID
CSCuz77293	OSPF 组播过滤器控制在集群从属设备中缺失
CSCuz80281	IPv6 邻居发现数据包处理行为
CSCuz87146	nat-t-disable 功能对 ikev2 不起作用
CSCuz89989	Ikev1 隧道丢失，原因为“Peer Address Changed”
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
CSCuz94158	内部对“Any”地址的散列计算出错
CSCuz94862	IKEv2：数据 rekey 冲突可能导致非活动 IPsec SA 卡住
CSCuz94890	在智能许可交换期间，先于所有数据收到 ASAv ACK FIN
CSCuz95703	仅管理 cli 在 QP-D 用户情景中不可用
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 消息处理程序而导致 CPU 使用率高
CSCva00939	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
CSCva02655	对于无客户端 VPN 流量，ASA 将无效的接口 ID 发送到 SFR

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
CSCva05513	ASA：SLA 控器无法与配置为非零的浮动超时配合使用
CSCva07268	在 ASA 升级后，无法通过无客户端进行第二次身份验证
CSCva10054	由于 sctp inspection，DATAPATH 中生成 ASA ASSERT 回溯
CSCva12520	snmpwalk 不适用于某些 NAT OID
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
CSCva24799	TLS 代理功能缺少客户端信任点命令
CSCva24924	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	线程名称 rtcli async executor process 出现 ASA 回溯
CSCva32092	OSPFv3/IPv6 在 ASA 集群和 4500 之间每隔 30 分钟就会摆动一次
CSCva35439	ASA DATAPATH 回读（集群）
CSCva36202	重新加载后，BGP 插槽在 ASA 上未打开
CSCva36884	思科 ASA 跨站点脚本 SSLVPN 漏洞
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
CSCva43746	ASA“show inventory”显示“Driver Error, invalid query ready”
CSCva43992	IKEv2 RA 证书身份验证。无法分配新的会话。已达到最大会话数目

警告 ID 号码	说明
CSCva45590	ASA OSPFv3 接口 ID 在启用/禁用故障切换时出现更改
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
CSCva50554	如果以不正确的配置引导，ASA 为主机 IP 地址使用“::”
CSCva50838	ASA capture type isakmp 不保存重组的 rfc7383 IKEv2 数据包
CSCva52514	ASAv Azure：asav 通过负载均衡器部署时，waagent 可能会重新加载
CSCva53581	增加全局 ARP 请求池
CSCva56114	CISCO-MEMORY-POOL-MIB 为 heapcache 返回不正确的值
CSCva56343	集群：由于 L2 条目超时，出现 TFW 异步流丢包
CSCva60283	Azure 中有针对 ASAv 的两个上游内核补丁
CSCva62667	ASP 路由表中显示关闭的接口
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
CSCva68364	替换 ASA 时，未重置 SNMPv3 的有效 engineID
CSCva68987	禁用 ICMP 检查时，ASA 丢弃 ICMP 请求数据包
CSCva69346	NAT 匹配时，无法从 ASA 中继 DHCP 发现数据包
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
CSCva70979	故障切换描述符在端口信道接口中未更新
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

警告 ID 号码	说明
CSCva77852	ipsecvpn-ikev2_oth：5525 9.4.2.11 在线程名称：IKEv2 Daemon 中生成回溯
CSCva81412	ASR9000 BGP 平稳重启未按预期运行
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
CSCva84625	ASAv 显示主机名生成智能许可授权请求
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)
CSCva86626	HTML5：Guacamole 服务器需要页面刷新
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
CSCva90419	issuer-name 错误地使用 attr 检测证书映射中的重复项
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
CSCva97863	971 EST - 执行 show capture 时控制台挂起
CSCva98240	SIP：从路由寻址：未正确转换报头
CSCva98532	FTD 内联未阻止 MPLS 交换的 TCP 会话，它应当阻止

警告 ID 号码	说明
CSCvb03994	IKE_DBG 中生成回溯
CSCvb04685	无法删除 SNMP 配置
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
CSCvb08776	在“show version”中错误地显示内部 ATA Compact Flash 大小
CSCvb13690	ASA：僵尸网络更新失败，且出现许多错误
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
CSCvb20256	ASA 的 SSH 实施中存在 Sweet32 漏洞
CSCvb21922	当未解析 FQDN 时，show access-lists 命令中显示 ACL 警告消息
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
CSCvb25139	启用 DNS 检测时，IPv6 DNS 数据包格式不正确。
CSCvb26119	Webvpn 重写程序在 matterport.com 上出现故障
CSCvb27868	ASA 1550 块因多情景透明防火墙而消耗
CSCvb28491	无法运行 show counters protocol ip
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	启用“基于策略的路由”后，ASA 可能生成 DATAPATH 生成回溯

警告 ID 号码	说明
CSCvb31055	ASA 多情景 SNMP PAT 接口缺失
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
CSCvb33009	思科 ASA 签名验证在引导时误导数字签名
CSCvb33013	思科 ASA 删除在非 SB 硬件上误导安全引导命令
CSCvb36199	运行 9.6.2 的线程名称：snmp ASA5585-SSP-2 生成回溯
CSCvb37456	在 IKE 重新生成密钥未能在主用设备上启动 ph1 重新生成密钥后出现故障切换
CSCvb38522	ASA PKI OCSP 失败 - CRYPTO_PKI：无法解码 OCSP 响应数据。
CSCvb39147	思科 ASA 平台上的 NFS 吞吐率降低
CSCvb40417	在 ASA“sh route”命令中看到 nlp_int_tap 路由
CSCvb40818	在 ipv6 命令中看到 nlp 信息
CSCvb40847	如果用户手动注销，则 ASA 不发送身份验证会话结束日志
CSCvb41097	GTPv2 丢失实例 1 切换
CSCvb43120	Checkheaps 线程中生成 ASA 回溯
CSCvb45039	线程名称 aaa_shim_thread 中生成 ASA 回溯
CSCvb46531	ASDM：ASAv 9.6.2 的内存使用率读取错误
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）
CSCvb49264	删除承载器请求无法在 v2 切换呼叫流后删除第二个默认承载器。
CSCvb49273	当来/往 ISE 发送/接收 CoA 时，CoA 会触发 ASA 上的生成回溯
CSCvb49445	IKEv2：在与客户端断开连接后，不清除会话。
CSCvb50301	ASA 在线程名称：rtcli 中生成回溯

警告 ID 号码	说明
CSCvb50609	RADIUS 授权请求不发送 Calling-Station-ID 属性
CSCvb50750	FTD 在具有 sip 流量的故障切换期间崩溃
CSCvb52157	viewer_dart.js 文件无法正确加载
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
CSCvb53094	ASA：为多情景防火墙使用的内存计算存在差异
CSCvb55721	使用站点 ip 地址的多站点集群中的 ASA 完成 GARP flood
CSCvb57817	EIGRP：获取按比例缩放的带宽时，需要添加大量错误处理
CSCvb58087	对象组搜索冗余服务对象被错误删除
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
CSCvb66593	url 中出现 webvpn_state cookie 信息泄露
CSCvb68766	线程名称：IKE Daemon 中生成 ASA 回溯。
CSCvb74084	SCP在 962 中失败
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
CSCvb75266	ASA - ACL 注释在 Packet Tracer 工具的 XML 输出中显示不正确
CSCvb75685	输入“no vpnclient enable”后，EZVPN NEM 客户端无法重新连接
CSCvb78614	4GE-SSM RJ45 接口可能会因接口“速率限制下降”而导致流量下降
CSCvb83446	解析 IE 失败时，v1 PDP 可能会被删除
CSCvb85624	对 CVE-2016-5195 (DIRTY CoW) 的 pix-asa 评估
CSCvb87586	在故障切换和插入/拔出后，无法连接 ssh 管理接口

警告 ID 号码	说明
CSCvb88126	ASA：尽管已修复 CSCuu48197，但卡住的 uauth 条目仍会拒绝 AnyConnect 连接
CSCvb88358	webvpn-l7-rewriter：5515 9.1.6 ASA Web 书签的内容重写问题
CSCvb89988	WebVPN：重写程序的内部页面的登录按钮不工作
CSCvb92125	ASA 因在重写期间超出标签长度而丢弃 DNS PTR 应答
CSCvb92417	集群 ASA 丢失传入 ICMP 回复，原因是“inspect-icmp-seq-num-not-matched”
CSCvb92548	在启用了对象组搜索的情况下，ASA 匹配错误的 ACL
CSCvb92823	当嵌入 NOTIFY 时，ASA SIP 检测可能延迟传输 200 OK，
CSCvc00015	在 ASA 集群的虚拟 IP 上进行 SNMP 轮询时，出现不正确的行为。
CSCvc00689	ASA：由于 ikev2 而发生内存泄漏
CSCvc00760	RDP 插件连接失败，并出现错误
CSCvc01685	PLR：ASAv 生成无效预留代码
CSCvc04741	ASA DHCP 中继与 intercept-dhcp 功能不兼容
CSCvc05005	ASA 集群 TCP/SSL 端口在 LISTEN 状态上不显示
CSCvc06150	ASA 无法在证书映射中添加多个属性条目
CSCvc07112	实现调度程序损坏问题的检测和自动修复功能
CSCvc07330	当运行 webvpn 时，ASAv 可能会崩溃
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
CSCvc16330	ASA-SM 9.5.2 inspect-sctp 许可中断现有部署
CSCvc19318	线程名称：sch_syslog 中生成 ASA 回溯
CSCvc22193	DSCP 标记未通过 IPsec 封装复制到外部 IP 报头

警告 ID 号码	说明
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
CSCvc25195	部署了 anyconnect 时，ASA 门户显示配置了多情景。
CSCvc25281	在重新启动集群设备后，同步 SNMPv3 用户时出错
CSCvc25409	当使用 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
CSCvc36535	在没有接口关闭后，在线程名称 ssh, rip igb_disable_rx_queues 中出现 ASA 回溯
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 的后端服务器之间中断
CSCvc38425	带 FirePOWER 模块的 ASA 生成回溯并重新加载或导致进程未运行
CSCvc39121	当 ASA 处于多情景模式下时，使用外部 DHCP 服务器进行 Anyconnect 地址分配失败
CSCvc44240	ASA 集群：在 9.6.2 中，mac-address cmd 在跨端口通道接口上被忽略
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 门户显示得不正确。
CSCvc52272	ASA 检查-MPF ACL 更改在 ASP 表中的排序不正确
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
CSCvc58272	ASA 错误地处理包装器中的负数，导致图形 webvpn 问题

警告 ID 号码	说明
CSCvc60254	SIP：含有多个段的 200 OK 消息重组错误
CSCvc60964	ASA L3 集群：在非对称路由的情况下，DHCP 中继丢失 DHCPOFFER
CSCvc61818	CTP 在尝试失败后，将域与用户名一起发送
CSCvc61845	RDP 插件 ActiveX 全屏选项在 ASA 9.6.2 版本中不可用
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
CSCvc79077	ASA watchdog 在启用了 rest-api 的 cluster config syn 期间生成回溯
CSCvc79371	未能正确更新 ASA nat 池。
CSCvc79454	无法为脚本用户配置 ssh public auth
CSCvc79569	mac-address auto 命令在 ASA5585-X 上使用默认前缀 1
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
CSCvc88115	ASA 集群 IDFW 不更新用户映射
CSCvc88411	由于 Radius Accounting 数据包而出现 1550 字节块损耗
CSCvc91839	由于 XML 解析错误，无法在 FTD 设备上部署策略
CSCvc93947	ASA(9.1.7.12)：通过备用 ASA 为组播流创建连接条目。
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
CSCvd03343	无法为非系统情景配置 SSH public key auth

警告 ID 号码	说明
CSCvd06022	升级后，ASA-FP9300 在线程名称 IPSEC MESSAGE HANDLER 中出现崩溃
CSCvd06527	SNMPv3 上行链路/下行链路应通过管理情景生成
CSCvd08200	ASA 中缓慢内存泄漏
CSCvd08479	ACL last hit-cnt 计数器显示不正确的时间
CSCvd08709	不对称路径 icmp 流量通过分布式集群失败
CSCvd14266	ASA 在 DATAPATH-41-16976 线程中生成回溯
CSCvd15843	当传递数据时，端口转发会话由于组策略中的“vpn-idle-timeout”而超时
CSCvd21154	在离开集群后的 30 秒，5585 不解绑其数据 intfs
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。
CSCvd26939	SNMP 为所有 FTD 受管设备列出同一主机名
CSCvd28859	ASA：ICMP 流量的 PBR 内存泄漏
CSCvd29150	管理路由删除还会移除数据平面路由。
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

警告 ID 号码	说明
CSCvd49262	尝试保存/查看具有巨型对象组 (display_hole_og) 的访问列表时出现回溯
CSCvd49550	当 managment0/0 用作 src-ip 时，9.5.1 及更高版本的 ASA 不显示 SXP 套接字
CSCvd50389	RT#687120：无客户端 VPN - SAML 存在书签问题
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
CSCvd58417	DCERPC 检测丢包并中断通信
CSCvd61308	由于 [Running Configurations] 错误，在多情景中的 ASA 备份失败
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 上公告
CSCvd65797	将 NAT 相关对象更改为 fqdn 时，ASA 可能崩溃
CSCvd66303	在 ESXi vCenter 6.5 上部署 ASAv 时出错
CSCvd69804	ASA - 接口状态更改导致使用 ipsec inner-routing-lookup 时 VPN 流量断开
CSCvd73468	由于空闲超时，集群目录连接超时
CSCvd76939	ASA 策略映射配置未复制到从属集群
CSCvd77893	ASA 可能在修改访问组时生成断言回溯
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

9.6(2) 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
CSCsh75522	内容长度计数器的字节大小从 4 增加到 8

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 达到峰值
CSCuh89500	ASA：SNMP 不为端口信道填充 ifSpeed/ifHighSpeed
CSCum70304	FIPS 自检开机故障 - fipsPostDrbgKat
CSCup37416	过时的 VPN Context 条目导致 ASA 停止对流量加密
CSCuu40736	捕获 <name> 类型线内标记接口，<name> 默认使用标记值 0
CSCuv09640	ASA：“Auto-Enable”功能不能与配置了 PKF 的 SSH 配合使用
CSCuw51576	SSH 连接在 ASA 上不超时（在 rtcli 中受阻）
CSCuw55813	线程名称 EIGRP IPv4 中出现备用 ASA 回溯
CSCux08783	CWS：ASA 不附加 XSS 报头
CSCux15273	show memory 指示的可用空闲内存不准确
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
CSCux33726	ASA 回溯 - WebVPN CIFS_file_rename_remove 操作
CSCux33974	ASA“show chunkstat | redirect”不工作
CSCux35538	在具有 DHE 密码 SSL VPN scaled test 的 ctm_ssl_generate_key 中生成回溯
CSCux39988	在透明模式下，故障切换对上出现不同的 BVI 地址输出
CSCux45179	SSL 会话停止处理 -“Unable to create session directory”错误
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
CSCux82023	由于 ASA 集群中回避/威胁检测，末节连接断开
CSCux82835	当启用 asp transactional-commit nat 时，观察到 nat 池耗尽
CSCux83705	对双堆栈的 DNS 回复修改未按预期运行
CSCux86769	当连接回退至 TLS 时，VLAN 映射不起作用

警告 ID 号码	说明
CSCux96716	设备加入集群时出现回溯
CSCux98029	ASA 重新加载，并在线程名称 DATAPATH 或 CP Processing 中生成回溯
CSCux99392	已通过 CIFS 上传/下载的文件大小为零字节（相同的 WebFolder）
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
CSCuy03024	引用线程名称 idfw_proc 时出现 ASA 回溯和重新加载
CSCuy05949	ASA：当发出 WRITE STANDBY 时主动情景中的 MAC 地址发生更改
CSCuy07753	自 Firefox 32 位版本 43 起，智能隧道不工作
CSCuy10665	HA：SFR 模块在两个设备上重新加载后，接口数不匹配
CSCuy11021	Webvpn 书签副标题不可见
CSCuy11281	ASA：版本 9.4.2 中生成断言回溯
CSCuy11905	在访问列表中提及用户名时，出现 ASA 5585 回溯
CSCuy13937	在 TLS 处理期间，CP Processing 线程中出现 ASA 监视器回溯
CSCuy15798	为 Radius 帐户数据包中的 IPv6 分配的地址字段添加支持
CSCuy18640	GTP 消息进程与 pdp 创建/删除之间存在潜在死锁
CSCuy19933	ASA 重写程序对类型为 <base>xxx</base> 的 HTML 代码的处理不正确
CSCuy21206	当 diameter inspection 和 tls-proxy 导致丢包时，会生成回溯
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
CSCuy30069	ASA 9.5.2 不为 512 位证书发送 CERT_REQ
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

警告 ID 号码	说明
CSCuy32964	无中断 fxos 升级期间出现机箱内 SSP ASA 集群回溯
CSCuy34265	配置更改后，ASA 访问列表丢失并丢失元素
CSCuy41986	当链中的多个证书已验证时，OCSP 验证失败
CSCuy42087	ASA：无法删除含“log default”关键字的 ACE
CSCuy42223	BGP：配置失败，原因为在仅管理接口上受支持
CSCuy43857	ASA WebVPN：Kronos 应用程序存在 Java 异常
CSCuy47706	Gtpv1_process_pdp_create_req 上生成回溯
CSCuy48237	无客户端 SSL VPN CIFS 压力测试：ramfs_webvpn_file_open 回溯
CSCuy49902	inspect ip-option 不允许“NOP”，即使被允许也是如此
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
CSCuy58084	无法仅为 ssh public auth（与 CSCuw90580 绑定在一起）配置用户
CSCuy59460	对于版本 3，对无效用户名的 SNMP 轮询会成功
CSCuy60320	IPv6 Routes 未安装在 QP 上
CSCuy62198	如果 FQDN 长度超过 64 个字符，我们会重新定向至 ip 而不是 FQDN
CSCuy63642	在 webvpn-datapath 中出现 ASA 9.1(6) 回溯：线程名称“DATAPATH-2-1524”
CSCuy65416	断言“ctm->async_ref == 0”失败：文件“ssl_common.c”，第 193 行第 2 部分
CSCuy65569	Coverity 114172：snp_fp_inspect_ip_options 中存在 FORWARD_NULL
CSCuy65571	Coverity 114170：parser_interface_list_invalid 中存在 SECURE_CODING
CSCuy67333	由于修复 CallId 与 Refer-To 之间的差异，SIP 呼叫转移失败
CSCuy68174	Coverity 114166：ss_send_health_check_request 中存在 NULL_RETURNS
CSCuy71812	Coverity 114217：snp_fp_action_cap_construct_key 中存在 NULL_RETURNS

警告 ID 号码	说明
CSCuy72255	Coverity 114176：oct_dbg_read_csr 中存在 CHECKED_RETURN
CSCuy72257	Coverity 114177：oct_dbg_write_csr 中存在 CHECKED_RETURN
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
CSCuy74362	WebVPN FTP 客户端出现故障，并显示消息“Error contacting host”
CSCuy78802	集群裂脑后，原主设备不会防御所有 GARP 数据包
CSCuy80058	FO 复制失败：禁用 webvpn-cache 时，cmd=no 禁用
CSCuy83792	Coverity 114304：ProcessConfiguration(vdi::config::Adi 中存在 CHECKED_RETURN
CSCuy84044	webworker JS 存在重写程序错误
CSCuy86333	BFD：ASA 可能在 snp_bfd_pp_process+101 中出现回溯
CSCuy87597	ASA - 在私钥解密期间 CP Processing 线程中生成回溯
CSCuy88971	ASA 不抑制 EIGRP 候选默认路由信息
CSCuy89425	AAA：RSA/SDI 无法设置新 PIN
CSCuy91405	ASA 不应通过端口信道 CCL 对相同的流量进行负载均衡
CSCuy91788	ASAv：可用内存在 OOM 情况下报告为负值
CSCuy94787	DATAPATH 中出现回溯或因威胁检测导致 CPU 利用率较高
CSCuy95543	提高 malloc_avail_freemem() 的效率
CSCuy96391	ASA 无客户端重写程序的“CSCOPut_hash”函数出现故障
CSCuy98769	在故障切换后，ASA OSPF 接口从 DOWN 过渡到 WAITING 的速度较慢
CSCuy99280	ENH：ASAv 应该有不同的预加载证书
CSCuz00077	ASA 9.1.6.4 在线程名称：telnet/ci 中生成回溯
CSCuz01658	带有重复请求的 gtp_remove_request 中出现回溯

警告 ID 号码	说明
CSCuz06125	仅配置了主用 MAC 时，主用和备用 ASA 使用相同的 MAC 地址
CSCuz06499	WebVPN：ASA 带有与 srv 相同的 FQDN 时，未完全重写网页
CSCuz08625	SSH 线程中出现 ASA 回溯
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
CSCuz14875	使用 address-family 子配置时，ASA RIP 出现崩溃
CSCuz16398	NAT 转移表修改错误
CSCuz16498	控制台上显示错误消息“ERROR: Problem with interface”
CSCuz18707	内联网页面不通过 WebVPN 加载，并出现 Javascript 错误
CSCuz20742	AWS：如果部署了 2 个接口，将无法访问 ASAv
CSCuz21068	CSCOPut_hash 会发起异常请求
CSCuz21178	线程名称 ssh 中生成 ASA 回溯
CSCuz23354	当 GTP 中的计时器离队失败后，CPU 使用率高
CSCuz23576	分配的内存显示较高（无效）的值
CSCuz27165	BTF 不阻止含超过 2 个标签、已列入黑名单的域
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
CSCuz34753	ASA QOS 无法在优先和最佳工作队列之间分类数据包
CSCuz36545	下拉菜单在 Simfosia 网页上不起作用
CSCuz36938	在编辑网络对象时，如果超出最大 snmp 主机数，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

警告 ID 号码	说明
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
CSCuz41033	如果命名与静态加密映射相同，则动态加密映射失败
CSCuz41308	在 show route 接口中显示区域密钥
CSCuz42390	DRP 的 ASA 有状态故障切换间歇性地工作
CSCuz42986	当 sfr 模块关闭时，ASA(HA) 不发送 RST 数据包
CSCuz50929	许多“show blocks”输出中含有截断的 PC 值和 ASLR
CSCuz52474	Pix-asa 的 Openssl 评估（2016 年 5 月）
CSCuz52859	从单模式转到多模式时，SNMPv3 noauth 陷阱/轮询不起作用
CSCuz53186	对 ASA AnyConnect CSTP 版权消息的更改不正确
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
CSCuz58142	ASA 访问列表缺失和丢失元素警告消息增强功能
CSCuz60555	内存不多时，可能收到无效的 ASA-2-321006
CSCuz61092	接口运行状况检查故障切换导致 OSPF 不向用作 ABR 的 ASA 通告
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
CSCuz66269	SCP 客户端不允许通过“no ssh stricthostkeycheck”输入密码
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

警告 ID 号码	说明
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
CSCuz70330	ASA：因为达到最大限制，SSH 在 ASA 设备上被拒绝
CSCuz72244	错误指示和空 TID MBReq 丢弃，没有 Ctrl F-TEID
CSCuz72352	tls-proxy 握手期间生成回溯
CSCuz77818	PIM BiDir DF 选举在一些接口上受阻于“offer”状态
CSCuz79800	ASA 无法删除 ACL 行和注释 - 指定的注释不存在
CSCuz81922	SRTS：“type”选项在“show cluster chassis xlate count”下缺失
CSCuz90648	2048/1550/9344 字节块泄漏导致通信中断和模块故障
CSCuz94862	IKEv2：数据 rekey 冲突可能导致非活动 IPsec SA 卡住
CSCuz98201	ASAv - CPU 利用率较高
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
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
CSCva02121	回溯线程名称 ci/console 调试菜单 ctm 103 导致 ASA 崩溃
CSCva02655	对于无客户端 VPN 流量，ASA 将无效的接口 ID 发送到 SFR
CSCva03982	ASA：集群模式中由于 PBR 查找发生内存泄漏
CSCva11580	ASA9.(6)1 回归“internal error”而不是“maximum time exceeded”
CSCva12520	snmpwalk 不适用于某些 NAT OID
CSCva12598	CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolHCFree.1.1 = Counter64：0 字节
CSCva14545	通过 oVirt 部署时无法启动 ASAv-KVM

警告 ID 号码	说明
CSCva26771	ASA：PBR 因数据包丢包而发生内存泄漏
CSCva35439	ASA DATAPATH 回读（集群）
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
CSCva45590	ASA OSPFv3 接口 ID 在启用/禁用故障切换时出现更改
CSCva62861	Uauth 在故障切换后失败
CSCva92151	思科 ASA SNMP 远程代码执行漏洞

9.6(1) 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。

标识符	描述
CSCtz98516	当查询 GET BULK 以获取“xlate count”时，在 SNMP 中观察到回溯
CSCuc11186	ARP：代理 IP 流量被劫持。
CSCun21186	从从属设备检索 idfw topn 用户时出现 ASA 回溯
CSCuo08193	在处理 nat-t 数据包时，线程名称 DATAPATH-1-1382 中出现回溯
CSCur46371	TLSv1.2 客户端证书身份验证连接设置故障
CSCur87011	低端 ASA-X -5512/5515 设备中 ASA 的 DMA 内存不足
CSCus10787	事务性 ACL 提交在编译期间将绕过安全策略
CSCus16416	共享许可证在重新启动后未在故障切换对上激活
CSCus53126	ASA 流量未使用“traffic-forward sfr monitor-only”正确发送
CSCut40770	接口 TLV 到 SFR 在帧长度超过 2048 字节时损坏
CSCut49034	ASA：由于 RDP 从 CL SSL 门户连接到 AC 客户端，备用设备上的 CPU 利用率较高
CSCut71095	ASA WebVPN 无客户端 cookie 身份验证绕行

标识符	描述
CSCuu02848	为 SSL 手动配置 RSA 证书时，禁用 ECDSA SSL 密码
CSCuu06081	ASAv 许可实施不应基于 CLI 解析器
CSCuu48197	ASA：受阻的 uauth 条目拒绝 AnyConnect 用户连接
CSCuu82229	具有 DH 19 及更高版本的 ikev2 无法在 phase2 重新生成密钥后传递流量
CSCuu91304	GET 断开 scansafe 连接后，立即从客户端获取 FIN
CSCuv20449	使用捕获或连续 ping 时，线程名称 ssh 中出现回溯
CSCuv49446	在线程 DATAPATH 中进行配置同步期间，备用设备上出现 ASA 回溯
CSCuv50709	在 Anyconnect 断开连接后，备用 ASA 内部 IP 会无法访问
CSCuv58559	在 MPF 中修改“set connection”时，线程名称 DATAPATH 中出现回溯
CSCuv66333	ASA 选择不正确的信任点来验证 OCSP 响应
CSCuv87150	线程名称 fover_parse (ak47/ramfs) 中出现 ASA 回溯
CSCuv87760	RAMFS 处理出现 Unicorn 代理线程回溯
CSCuv92371	ASA 回溯：SSH 线程：许多用户已登录且正在修改 dACL
CSCuv92384	ASA TCP 规范化程序为半开 CONNS 的无效 ACK 发送 PUSH ACK
CSCuv94338	线程名称 CP Crypto Result Processing 中出现 ASA 回溯。
CSCuw02009	ASA - SSH 会话在 CLOSE_WAIT 中受阻，导致 ASA 发送 RST
CSCuw09578	进行 WebVPN 压力测试时，在 ak47_platform.c 中出现 ASA 9.3.3.224 回溯
CSCuw14334	线程名称 IP Address Assign 出现回溯
CSCuw16607	ASA EIGRP 不通过为邻居发送毒性逆转来删除路由
CSCuw17930	对远程重叠网络进行不正确的 S2S IPSec 数据路径选择
CSCuw19671	从 ASDM 恢复备份配置时出现 ASA 回溯
CSCuw22130	从集群删除动态 PAT 语句时出现 ASA 回溯
CSCuw22886	拆分隧道对于 Kenton 设备 (9.5.1) 上 EzVPN 客户端不起作用

标识符	描述
CSCuw24664	ASA：线程名称 netfs_thread_init 中出现回溯
CSCuw26991	ASA：线程 Unicorn 管理处理程序因威胁检测而出现回溯
CSCuw28735	思科 ASA 软件版本信息泄露漏洞
CSCuw29566	ASA5585 9.5(1)：在 Management0/0 端口上支持故障切换局域网
CSCuw33860	RA-VPN 事务在 PRSM 控制面板中显示为 0
CSCuw36853	ASA：在具有接口 PAT 的集群 CCL 上出现 ICMP 错误循环
CSCuw39685	过滤器 sfr 流量可能导致内存损坏
CSCuw41548	channel_put() 中出现 DNS 回溯
CSCuw44038	含有大量 ldap grps 的 ldap_client_thread 中出现监视器回溯
CSCuw44744	WebVPN 重写程序出现回溯
CSCuw48499	QEMU coredump：qemu_thread_create：资源暂时不可用
CSCuw51576	SSH 连接在备用 ASA 上未超时（在 rtcli 中受阻）
CSCuw55813	线程名称 EIGRP IPv4 中出现备用 ASA 回溯
CSCuw59388	在多情景模式下无法将 ASDM 加载到某个情景
CSCuw66397	如果已从 CLI 启用 dhcpd auto_config，则 DHCP 服务器进程受阻
CSCuw85261	SAML 无法选择 Oracle OAM 隧道组
CSCuw86069	ASAv 无法删除/更改默认的 global_policy 或 inspection_default
CSCuw87331	ASA：线程名称 DATAPATH-7-1918 中出现回溯
CSCuw87910	访问页面时，PCP 10.6 无客户端 VPN 访问被拒绝
CSCuw90116	在清除和重新配置 ACL 时出现 ASA 9.4.1 回溯
CSCuw92005	线程名称：DATAPATH-17-3095：ASA 在集群中意外重新加载
CSCux03626	在线程名称 Unicorn Proxy Thread 中出现回溯
CSCux05081	RSA 4096 密钥生成导致故障切换

标识符	描述
CSCux07002	ASA：断言“pp->pd == pd”失败：文件“main.c”，第 192 行
CSCux08783	CWS：ASA 不附加 XSS 报头
CSCux09181	在 9.3.2 后，http 形式的身份验证失败
CSCux09310	使用 ECDSA 证书时出现 ASA 回溯
CSCux15273	show memory 指示的可用空闲内存不准确
CSCux16427	对 deny 子句的 PBR 路由选择不正确
CSCux20178	在 9.2 及更高版本中，OSPF 邻居在“reload in xx”命令后关闭
CSCux21955	ASA：FAILOVER 与密码加密无法配合使用。
CSCux23659	在删除 Compact Flash 并执行 dir 命令后，ASA 9.1.6.10 出现回溯
CSCux29929	ASA 9.4.2 在 DATAPATH 中生成回溯
CSCux30780	gtpv1_process_msg 中出现 GTPv1 回溯
CSCux36112	PBR：在集群模式下由于基于策略的路由出现内存泄漏
CSCux37303	Gi 0/0 上的端口信道配置导致引导循环 - 与 FIPS 相关
CSCux37442	ASA 上 WebVpn 端口转发二进制的思科签名证书已过期
CSCux41145	针对 2015 年 12 月 OpenSSL 漏洞的 pix-asa 评估
CSCux42936	线程名称 Datapath 中由于 SIP 检测出现 ASA 9.5.1 回溯
CSCux43978	DHCP 中继因集群 ASA 的接口名称太长而失败
CSCux45179	SSL 会话停止处理 -“Unable to create session directory”错误
CSCux47195	ASA(9.5.2) 更改发送给具有 SFR 重新定向的客户端的 ACK 编号
CSCux56111	“no ipv6-vpn-addr-assign”CLI 不工作
CSCux59122	ASA L7 策略映射仅在重新应用检测后才起作用
CSCux61257	ASA：线程 IP 地址分配出现回溯
CSCux69987	ASA：在 NAT 规则中添加 FQDN 对象后，ASA 设备上出现回溯

标识符	描述
CSCux70998	在线程名称 IKE Daemon 中出现重新加载
CSCux71197	“show resource usage”在 sh shut/no 后提供错误路由数
CSCux72610	ASA TACACS+：进程 tacplus_snd 的 CPU 使用百分比较高
CSCux72835	ASA 9.5 - OCSP 检查使用全局路由表而不是管理
CSCux81683	线程名称 Unicorn Admin Handler 中出现 ASA 回溯
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
CSCux87457	线程名称 netfs_thread_init 中出现 ASA 回溯
CSCux88237	DATAPATH 线程中出现 ASA 回溯
CSCux93751	思科 ASA Linux 内核漏洞 - CVE-2016-0728
CSCuy01420	线程名称 Unicorn Proxy Thread 中出现 ASA 回溯。
CSCuy03024	引用线程名称 idfw_proc 时出现 ASA 回溯和重新加载
CSCuy11905	在访问列表中提及用户名时，出现 ASA 5585 回溯
CSCuy13937	在 TLS 处理期间，CP Processing 线程中出现 ASA 监视器回溯
CSCuy22561	VPN Load-Balancing 不发送 Ipv6 地址的负载均衡证书
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
CSCuy41986	当链中的多个证书已验证时，OCSP 验证失败
CSCuy47706	Gtpv1_process_pdp_create_req 上生成回溯

最终用户许可证协议

有关最终用户许可证协议的信息，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。