应用服务网格

服务公告

文档版本 05

发布日期 2026-06-16

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 Istio 版本支持机制

应用服务网格（ASM，Application Service Mesh）以原生的Istio为核心，提供高性能、高可靠性和易用性的全托管服务网格，以基础设施的方式为用户提供服务流量管理、服务运行监控、服务访问安全以及服务发布能力。社区定期发布Istio版本，ASM会随之发布相应的Istio版本。本文将为您介绍ASM服务的Istio版本策略。

表 1-1 ASM 服务 Istio 版本生命周期表

版本号	状态	社区发布时间	版本公测时间	版本商用时间	版本EOS（停止服务）时间
v1.28	公测	2025年11月	2026年2月	2026年10月	2028年10月
v1.18	已商用	2023年6月	2023年12月	2024年6月	2027年6月
v1.15	已商用	2022年8月	2023年4月	2023年10月	2026年10月
v1.13	EOS	2022年2月	2022年6月	2023年1月	2026年1月
v1.8	EOS	2021年5月	2021年7月	2022年1月	2024年4月
v1.6	EOS	2020年5月	2020年9月	2021年5月	2024年4月
v1.3	EOS	2019年9月	2019年12月	2020年3月	2024年4月

ASM 服务 Istio 版本阶段说明

- 版本公测阶段：您可以通过Istio公测版本体验最新的Istio版本特性，但需要注意该版本的稳定性未得到完全的验证。
- 版本商用阶段：商用版本经过充分验证，稳定可靠。
- 版本EOS（停止服务）阶段：Istio版本EOS之后，ASM服务将不再支持对该Istio版本的创建，同时不提供相应的技术支持，包含新特性更新、漏洞/问题修复、补丁升级以及工单指导、在线排查等客户支持。

ASM 服务 Istio 版本号说明

Istio的版本号基于社区Istio版本迭代演进，因此版本号由社区Istio版本和补丁版本两部分共同构成，格式为vX.Y.Z-rN（例如v1.28.2-r0）：

- Istio版本：格式为**X.Y.Z**，继承社区版本策略，其中**X**对应社区Istio的主要版本，**Y**对应社区Istio的次要版本，**Z**对应社区Istio的补丁版本，详情请参见**社区Istio版本策略**。
- 补丁版本：格式形如v1.28.2-**rN**，处于维护期的Istio版本会不定期地发布新的补丁版本。当新的补丁版本较上一版本提供了新的特性、Bugfix、漏洞修复或场景优化时，**N**版本号增加。

ASM 服务 Istio 版本升级

为了方便您体验新特性、规避已知漏洞/问题，使用安全、稳定、可靠的Istio版本，建议您定期升级Istio版本。Istio版本EOS（停止服务）之后，您将无法获得相应的技术支持，请您务必及时升级版本。 网格升级到新版本后，不支持回退到老版本。

ASM 服务 Istio 与 CCE 集群版本兼容关系

本文为您介绍应用服务网格（ASM）的Istio版本支持机制。

表 1-2 ASM 服务 Istio 与 CCE 集群版本兼容关系

Istio版本	配套的CCE集群版本
v1.28	v1.30、v1.31、v1.32、v1.33、v1.34、v1.35
v1.18	v1.25、v1.27、v1.28、v1.29、v1.30、v1.31、v1.32、v1.33、v1.34、v1.35
v1.15	v1.21、v1.23、v1.25、v1.27、v1.28
v1.13	v1.21、v1.23
v1.8	v1.15、v1.17、v1.19、v1.21
v1.6	v1.15、v1.17
v1.3	v1.13、v1.15、v1.17、v1.19

2 漏洞公告

2.1 未认证的控制面 DoS 攻击（CVE-2022-23635）

漏洞详情

表 2-1 漏洞信息

漏洞类型	CVE-ID	披露/发现时间
DoS	CVE-2022-23635	2022-02-22

影响评分

7.5 高危

触发场景

- 简单安装时，Istiod是从集群内获取的，受攻击的可能性小一点。
- 多集群场景安装的时候，15012端口是暴露在公网的，受攻击影响的可能性大一些。

根本原因

15012端口接收的请求不需要认证信息即可被Istiod处理，在大量向Istiod该端口发送请求时会导致Istiod服务不可用。

受影响版本

低于1.13.1版本的Istio

补丁修复版本

- ASM 1.8.4-r5版本及以上

- Istio 1.13.1版本及以上
- Istio 1.12.4版本及以上
- Istio 1.11.7版本及以上

规避和消减措施

除了升级版本没有有效的规避措施。将客户端对Istiod的网络访问限制在最小范围可以帮助减少某种程度上的漏洞的影响范围。

相关链接

- Istio官方**安全公告**
- Istio社区**漏洞公告**

2.2 Istiod TLS 证书密钥滥用（CVE-2021-34824）

漏洞详情

表 2-2 漏洞信息

漏洞类型	CVE-ID	披露/发现时间
TLS证书密钥滥用	CVE-2021-34824	2021-06-24

影响评分

9.1 高危

触发场景

同时满足下列三个条件：

1. Istio版本为1.8.x，或1.10.0-1.110.1，或1.9.0-1.9.5
2. Gateways或DestinationRules资源中定义了credentialName字段
3. 没有将Istiod flag置为PILOT_ENABLE_XDS_CACHE=false

根本原因

Istio Gateway和DestinationRule可以通过credentialName配置从Kubernetes Secret中加载私钥和证书。对于Istio1.8及更高版本，Secret通过XDS API从Istiod传送到网关或工作负载。

网关或工作负载部署应该只能访问存储在其命名空间内的Kubernetes Secret中的凭证（TLS证书和私钥）。但是，Istiod中的一个错误允许授权客户端访问和检索缓存在Istiod中的任何TLS证书和私钥。

受影响版本

参考**触发场景**

补丁修复版本

- ASM 1.8.4-r5版本及以上
- Istio 1.10.2版本及以上
- Istio 1.9.6版本及以上

规避和消减措施

除了升级版本来规避外，还可以通过设置Istiod的环境变量PILOT_ENABLE_XDS_CACHE=false来关闭Istiod缓存。但是，在关闭了XDS缓存后，系统和Istiod的性能可能会受影响。

相关链接

- Istio官方**安全问题汇总**
- CVE**漏洞公告**

2.3 HTTP/2 Bomb 远程拒绝服务漏洞（CVE-2026-47774）

漏洞详情

表 2-3 漏洞信息

漏洞类型	CVE-ID	披露/发现时间
HTTP/2 远程拒绝服务	CVE-2026-47774	2026-06-05

影响评分

7.5 高危

触发场景

同时满足下列两个条件：

- 受影响版本如下表：

表 2-4 版本列表

版本范围	状态
ASM 1.28.2-r2 及以下	受影响
ASM 1.18.7-r7 及以下	受影响
ASM 1.15.7-r6 及以下	受影响
ASM 1.3/1.6/1.8/1.13所有版本	受影响

- 通过Gateway暴露HTTP/2 或 gRPC 服务到公网

根本原因

在HTTP/2请求处理过程中，cookie头字段会被分片分别缓存，只有在完成请求头大小校验之后才会合并。由于这些缓存的cookie字节并未完全计入有效请求头的大小检查，超大cookie数据可以绕过 max_request_headers_kb 的限制。

另外，oghttp2/quiche 对编码后的 HPACK 字节数施加头块长度限制，而非针对完全解码后的头大小。恶意客户端可以利用这一不对称性，通过使用动态表引用使编码后的表示形式保持较小，同时导致解码后的cookie头值在内存中变得大得多。

当这两种行为结合在一起时，客户端可以迫使Envoy为每个流分配大量的内存。在持续的并发请求下，这会迅速增加进程的内存使用量，最终导致内存溢出（ OOM ）终止。

流量控制阻塞可进一步延长流的生命周期并推迟每流内存的回收，从而增强攻击的效果。

受影响版本

参考**触发场景**

补丁修复版本

表 2-5 修复版本

版本范围
ASM 1.28.2-r3 及以上
ASM 1.18.7-r8 及以上
ASM 1.15.7-r7 及以上

规避和消减措施

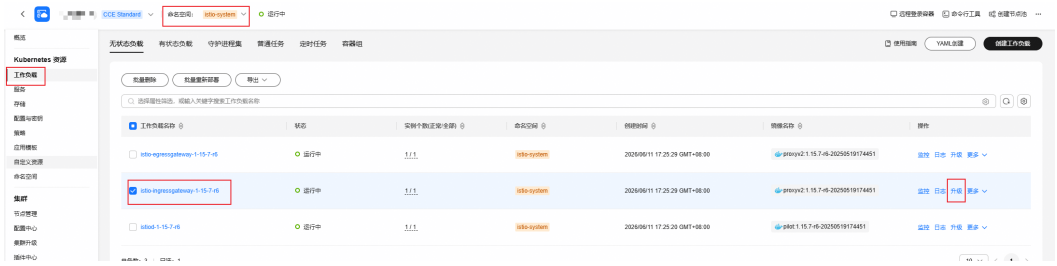
当前请通过升级Istio-Ingressgateway来消减风险。请注意，如果您使用1.15以下的EOS版本，需升级到1.15及以上版本再执行规避方案。

操作步骤

步骤1 登录**应用服务网格控制台**，单击服务网格的名称，进入网格详情页面。在网格详情界面，在左侧导航栏选择“网格配置”，单击“基本信息”页签，确认网格所属集群。

步骤2 登录**CCE控制台**。进入对应的CCE集群详情界面。

步骤3 在左侧导航栏选择工作负载，命名空间选择istio-system，找到istio-ingressgateway-{网格版本}的工作负载，单击升级。



步骤4 在升级配置页面中，选择**容器配置 > 容器信息**。

步骤5 在**镜像版本**字段中，根据网格版本按**表2-6**选择目标镜像版本。

表 2-6 网格版本对应的镜像版本规则

网格版本	镜像版本
1.15	1.15.7-r7-20260611204502
1.18	1.18.7-r8-20260611204441
1.28	1.28.2-r3-20260612154216

步骤6 单击升级工作负载。

注意

升级Istio-ingressgateway会造成网关实例滚动重启，可能会造成业务中断，请评估业务影响并选择合适的时间执行。

----结束

相关链接

- Istio官方**安全问题汇总**
- CVE**漏洞公告**

3 产品公告

3.1 Istio Operator 保留用户关键运行配置说明

服务公告

Istio采用Istio Operator安装的场景下，有时需要更新被Istio Operator管理的组件（包括istiod、istio-ingressgateway、istio-egressgateway）的工作负载，在低版本的ASM中，Istio Operator组件重启，可能会导致部分用户运行配置被重置为默认值，建议及时升级ASM版本以避免对您的业务产生影响。

触发场景

ASM使用IstioOperator的CRD资源对网格组件进行配置，在1.8.4版本中，用户若通过CCE控制台“工作负载”页面**修改IstioOperator默认关键配置**，Istio Operator组件重启会刷新用户的配置，导致用户所配置的如副本数、调度策略、资源限制等被默认配置覆盖。

影响范围

ASM 1.8.4所有版本。

建议措施

为了避免多个入口的配置相冲突，以及确保Istio各工作负载持续稳定运行，建议将ASM实例升级至1.8.6或以上版本，具体操作请参见**升级网格**。升级后**Istio Operator将对关键配置**进行保护。

3.2 ASM 企业版关闭创建入口说明

服务公告

停售时间：2024/4/30

华为云ASM企业版于2024/4/30 00:00:00（北京时间）停售，停售后ASM不再提供创建新企业版网格的能力，存量的企业版网格1.8版本也于2024/04/30 00:00（北京时

间）正式**停止维护**，建议您尽快迁移到基础版网格。关于如何迁移到基础版网格，请参见**1.0企业版网格迁移到基础版概述**。

3.3 ASM 关于 istio-system、istio-operator 命名空间下重要系统资源修改风险说明

服务公告

ASM使用istio-system、istio-operator命名空间承载网格运行所需的系统组件和系统运行配置，对于其下的资源对象：

- istio-system命名空间中的Deployment、DaemonSet、Service、ConfigMap、Secret、Role、RoleBinding、ServiceAccount资源对象；
- istio-operator命名空间下的Deployment、IstioOperator、ConfigMap、Secret、Role、RoleBinding、ServiceAccount资源对象；

建议您谨慎根据应用服务网格**官网资料文档**或在相关技术支持的指导下进行修改操作，以避免对您的业务产生影响。若用户有特定需求，也可通过**提交工单**进行咨询。

3.4 ASM 服务支持细粒度权限控制说明

服务公告

ASM服务已支持使用IAM进行细粒度权限控制，当使用非管理员账号登录并操作ASM服务时，需要对子账号进行授权，才能正常使用ASM服务。如果您当前通过IAM对用户进行权限管理，建议及时配置ASM相关权限避免对你的正常使用产生影响。

如果您之前使用CCE Action进行ASM服务的细粒度权限控制，这些配置也已失效，建议及时配置ASM相关权限避免对你的正常使用产生影响。

触发场景

用户通过IAM对用户进行权限管理，并且使用非管理员账号登录华为云，操作ASM服务。

建议措施

请参考详细的**权限管理**配置，以确保正确实施并满足您的具体需求。

4 网格版本公告

4.1 1.3 版本网格停止维护公告

发布时间：2024/04/24

华为云ASM网格1.3版本即将于2024/04/30 00:00（北京时间）正式停止维护，届时针对ASM网格1.3以及之前的版本，华为云将不再支持新网格创建。若您账号下存在1.3及之前的网格版本，为了保证您的服务权益，建议尽快升级到最新的商用版本。关于如何升级网格，请参见ASM**升级网格**指导。关于ASM不同网格的版本特性，请参见**版本特性**说明。

4.2 1.6 版本网格停止维护公告

发布时间：2024/04/24

华为云ASM网格1.6版本即将于2024/04/30 00:00（北京时间）正式停止维护，届时针对ASM网格1.6以及之前的版本，华为云将不再支持新网格创建。若您账号下存在1.6及之前的网格版本，为了保证您的服务权益，建议尽快升级到最新的商用版本。关于如何升级网格，请参见ASM**升级网格**指导。关于ASM不同网格的版本特性，请参见**版本特性**说明。

4.3 1.8 版本网格停止维护公告

发布时间：2024/04/24

华为云ASM网格1.8版本即将于2024/04/30 00:00（北京时间）正式停止维护，届时针对ASM网格1.8以及之前的版本，华为云将不再支持新网格创建。若您账号下存在1.8及之前的网格版本，为了保证您的服务权益，建议尽快升级到最新的商用版本。关于如何升级网格，请参见ASM**升级网格**指导。关于ASM不同网格的版本特性，请参见**版本特性**说明。

4.4 1.13 版本网格停止维护公告

发布时间：2026/06/08

华为云ASM服务网格1.13版本于2026/01/31 00:00（北京时间）正式停止维护，届时针对ASM网格1.13以及之前的版本，华为云将不再支持新网格创建。若您账号下存在1.13及之前的网格版本，为了保证您的服务权益，建议尽快升级到最新的商用版本。关于如何升级网格，请参见ASM**升级网格**指导。关于ASM不同网格的版本特性，请参见**版本特性**说明。

4.5 1.15 版本网格停止创建公告

停止创建时间：2026/01/30

华为云ASM网格1.15版本即将于2026/01/30 00:00（北京时间）正式停止创建功能，存量用户不受影响，可继续正常使用。关于ASM不同网格的版本特性，请参见**版本特性**说明。