应用服务网格

服务公告

文档版本 01

发布日期 2023-05-30

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

本文为您介绍应用服务网格（ASM）的Istio版本支持机制。

版本支持

- 网格维护

  ASM最多同时支持Istio三个大版本的维护。假设现存维护的是v1.17、v1.15、v1.13三个版本。当v1.18版本商用后，之前较早的版本v1.13将被停用。

版本约束

网格升级到新版本后，不支持回退到老版本。

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**

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，具体操作请参见用户指南-网格配置-升级。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

华为云ASM企业版计划于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，存量企业版网格可继续使用和续订。企业版能力将迁移至**华为云UCS服务**在UCS多云治理的大框架下为客户提供统一的全域流量治理能力。

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。