Application Service Mesh

Product Bulletin

Issue	02
Date	2024-04-30

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Istio Version Support Mechanism

This section describes the Istio version support mechanism of Application Service Mesh (ASM).

Version Requirements

- Mesh maintenance

  ASM supports the maintenance of a maximum of three major Istio versions at the same time. Assume that v1.17, v1.15, and v1.13 are maintained. After v1.18 is commercially available, v1.13 will be suspended.

Version Constraints

After a mesh is upgraded, it cannot be rolled back to the source version.

2 Vulnerability Notices

2.1 Unauthenticated Control Plane DoS Attack (CVE-2022-23635)

Description

Table 2-1 Vulnerability information

Vulnerability Type	CVE-ID	Discovered
DoS	CVE-2022-23635	2022-02-22

Impact Score

7.5 (high risk)

Trigger Conditions

- For simple installations, Istiod is typically only reachable from within the cluster, limiting the blast radius.
- For multi-cluster installations, port 15012 is exposed over a public network.

Root Cause

Istiod can process requests received on port 15012 even without authentication information. However, if there are too many requests sent to this port, Istiod will become unavailable.

Affected Versions

Istio earlier than 1.13.1

Patches

- ASM 1.8.4-r5 or later
- Istio 1.13.1 or later
- Istio 1.12.4 or later
- Istio 1.11.7 or later

Workarounds

There are no effective workarounds, beyond upgrading. Limiting network access to Istiod to the minimal set of clients can help lessen the scope of the vulnerability to some extent.

Helpful Links

- Istio official website: **Security Notice**
- Istio community: **Vulnerability Notice**

2.2 Istiod TLS Certificate and Private Key Abuse (CVE-2021-34824)

Description

Table 2-2 Vulnerability information

Vulnerability Type	CVE-ID	Discovered
TLS certificate and key abuse	CVE-2021-34824	2021-06-24

Impact Score

9.1 (high risk)

Trigger Conditions

Your cluster will be impacted if the following conditions are met:

1. The Istio version is 1.8.x, 1.10.0-1.110.1, or 1.9.0-1.9.5.
2. The **credentialName** field is defined in Gateways or DestinationRules.
3. The Istiod flag is not set to P**ILOT_ENABLE_XDS_CACHE=false**.

Root Cause

Istio Gateway and DestinationRule can load private keys and certificates from Kubernetes secrets through the **credentialName** configuration. For Istio 1.8 and later versions, secrets are transferred from Istiod to gateways or workloads through the XDS API.

In the above approach, a gateway or workload deployment should only be able to access credentials (TLS certificates and private keys) stored in the Kubernetes secrets within its namespace. However, a bug in Istiod permits an authorized client the ability to access and retrieve any TLS certificate and private key cached in Istiod.

Affected Versions

For details, see **Trigger Conditions**.

Patches

- ASM 1.8.4-r5 or later
- Istio 1.10.2 or later
- Istio 1.9.6 or later

Workarounds

Update your cluster to the latest version. If an upgrade is not feasible, this vulnerability can be mitigated by disabling Istiod caching. Caching is disabled by setting an Istiod environment variable **PILOT_ENABLE_XDS_CACHE=false**. However, system and Istiod performance may be impacted as this disables XDS caching.

Helpful Links

- Istio official website: **Summary of Security Issues**
- CVE **Vulnerability Notice**

3 Product Notices

3.1 Retaining Key Running Configurations of Istio Operator

Service Notice

If Istio is installed using Istio Operator, the workloads of components (istiod, istio-ingressgateway, and istio-egressgateway) managed by Istio Operator need to be updated. In ASM of an earlier version, if the component is restarted, your running configurations may be reset to the default values. You are advised to upgrade the ASM version in a timely manner to avoid impacts on your services.

Trigger Conditions

ASM uses CRD resources of Istio Operator to configure mesh components. In ASM 1.8.4, if you **modify the default key configuration of Istio Operator** on the **Workloads** page in CCE, the configuration will be updated when Istio Operator restarts. The default configurations, such as the number of copies, scheduling policy, and resource limit, are also be overwritten.

Affected Versions

All ASM 1.8.4 versions.

Workarounds

To avoid configuration conflicts between multiple entries and ensure continuous and stable running of Istio workloads, you are advised to upgrade the ASM instance to 1.8.6 or later. For details, see **Upgrading a Mesh**. After the upgrade, **Istio Operator protects key configurations**.

4 Mesh Version Notices

4.1 End of Maintenance for ASM 1.3

Released: April 24, 2024

Huawei Cloud ASM 1.3 will be end of maintenance (EOM) on April 30, 2024, 00:00 GMT+08:00. By then, you cannot create meshes 1.3 and earlier versions. Upgrade your mesh 1.3 and earlier versions to the latest commercial version. For details about how to upgrade a mesh, see **Upgrading a Mesh**. For details about the version features of different mesh editions, see **Version Features**.

4.2 End of Maintenance for ASM 1.6

Released: April 24, 2024

Huawei Cloud ASM 1.6 will be end of maintenance (EOM) on April 30, 2024, 00:00 GMT+08:00. By then, you cannot create meshes 1.6 and earlier versions. Upgrade your mesh 1.6 and earlier versions to the latest commercial version. For details about how to upgrade a mesh, see **Upgrading a Mesh**. For details about the version features of different mesh editions, see **Version Features**.

4.3 End of Maintenance for ASM 1.8

Released: April 24, 2024

Huawei Cloud ASM 1.8 will be end of maintenance (EOM) on April 30, 2024, 00:00 GMT+08:00. By then, you cannot create meshes 1.8 and earlier versions. Upgrade your mesh 1.8 and earlier versions to the latest commercial version. For details about how to upgrade a mesh, see **Upgrading a Mesh**. For details about the version features of different mesh editions, see **Version Features**.

