H3C CAS 不涉及Istio敏感信息泄露漏洞(CVE-2021-34824)

H3Cloud CAS CVM CVK 吕喜庆 2021-06-30 发表

漏洞描述

Istio 是一个由谷歌、IBM等共同开发的开源服务网格，该网格具有负载均衡、服务间认证、监控等功能，而不需要对服务的代码做任何改动，是开展云网格技术和智能微服务管理的一个很好方式。istio适用于容器或虚拟机环境（特别是 k8s）以及兼容异构架构。近日，Istio官方发布了安全公告，公布了Istio存在的敏感信息泄露漏洞，漏洞编号CVE-2021-34824，漏洞威胁等级：严重。

一、 漏洞描述

Istio Gateway DestinationRule 可以通过从 Kubernetes 私密内容中加载私钥和证书配置（TLS证书和私钥）。当Istio满足已定义Gateways且DestinationRules具有credentialName 指定的字段以及Istiod 的环境参数为PILOT_ENABLE_XDS_CACHE=false的条件时候，攻击者可利用该漏洞存在的错误授权，通过 XDS API 从 Istiod 传送私密文件到网关或工作负载；该行为导致攻击者可以借此窃取到证书和私钥信息，并借此接管 k8s 集群。

一、 影响范围

Istio 1.10.0 - 1.10.1
Istio 1.9.0 - 1.9.5
Istio 1.8.x

漏洞解决方案

H3C CAS 未使用上述组件，不涉及该漏洞。