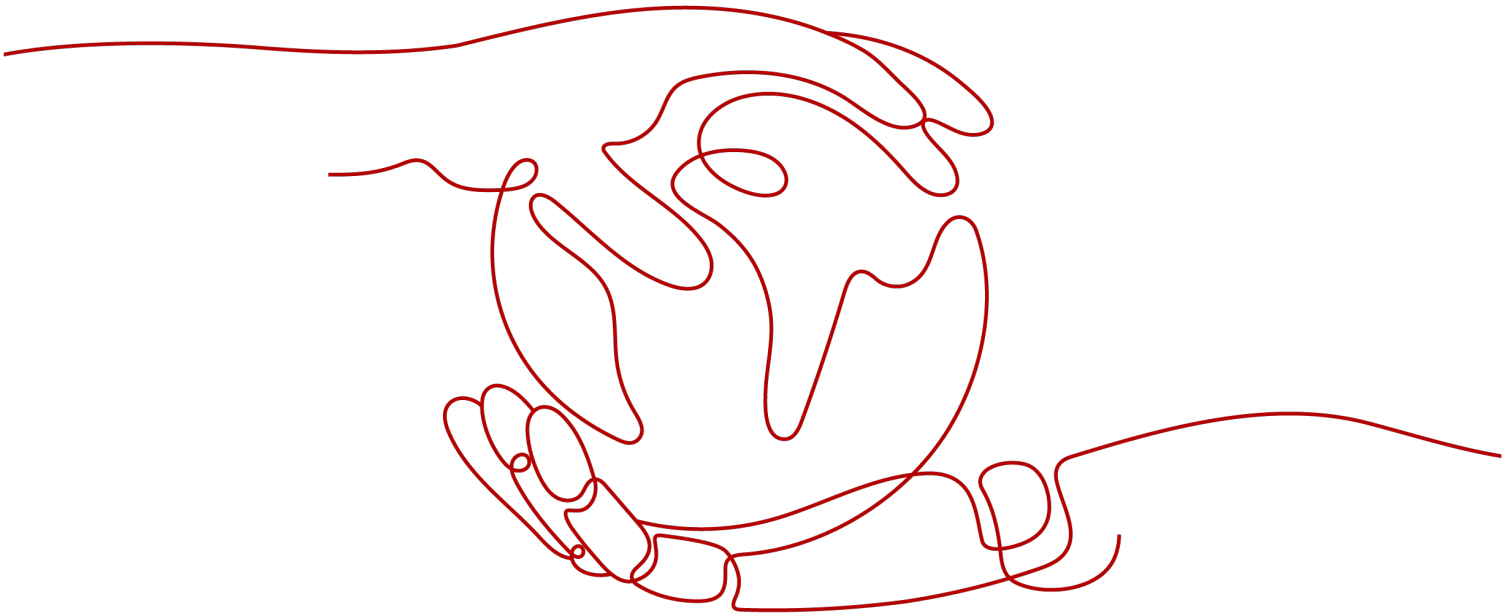
华为云 UCS

服务公告

文档版本 01

发布日期 2025-02-20



华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 漏洞公告

1.1 HTTP/2 协议拒绝服务漏洞公告（CVE-2023-4487）

漏洞详情

此漏洞允许恶意攻击者发起针对HTTP/2 服务器的DDoS攻击，使用 HEADERS 和 RST_STREAM发送一组HTTP请求，并重复此模式以在目标 HTTP/2 服务器上生成大量流量。通过在单个连接中打包多个HEADERS和RST_STREAM帧，显著提升每秒请求量，提升服务器上的CPU利用率，从而导致由于资源消耗造成的服务器拒绝服务。

表 1-1 漏洞信息

漏洞名称	CVE-ID	漏洞级别	披露/发现时间
HTTP/2 协议拒绝服务漏洞	**CVE-2023-44487**	高	2023-10-10

漏洞影响

此漏洞为拒绝服务类型漏洞，不影响数据安全，但恶意攻击者可能通过此漏洞造成服务器拒绝服务，导致服务器宕机。

漏洞修复方案

请在VPC内做好安全组加固，确保仅暴露接口给受信用户。

参考链接

HTTP/2协议拒绝服务漏洞

附：为何影响?

HTTP/2 允许在单个连接上同时发送多个请求，每个 HTTP 请求或响应使用不同的流。连接上的数据流被称为数据帧，每个数据帧都包含一个固定的头部，用来描述该数据帧的类型、所属的流 ID 等。一些比较重要的数据帧类型如**表1-2**所示。

表 1-2 重要数据帧介绍

名称	作用
SETTINGS帧	用于传递关于HTTP2连接的配置参数。
HEADERS帧	包含 HTTP headers。
DATA帧	包含 HTTP body。
RST_STREAM帧	直接取消一个流。客户端可以通过发送RST_STREAM帧直接取消一个流，当服务端收到一个RST_STREAM帧时，会直接关闭该流，该流也不再属于活跃流。

假设当前 TCP 连接设置的最大并发流数目为 1，那么当客户端发送请求1后，马上发送请求2，此时Server并不会真正处理请求2，而是直接响应RST_STREAM。因此，如果客户端在发送请求后紧接着发送RST_STREAM，就可以不停地向Server发送请求且不用等待任何响应，而Server则会陷入不停地接收请求-处理请求-直接结束请求的循环中，这个过程会消耗部分系统资源。

从而，恶意攻击者就可以利用该漏洞，通过持续的HEADERS、RST_STREAM帧组合，消耗 Server 资源，进而影响 Server 对正常请求的处理，造成 DDoS 攻击。

说明

- 最大并发流数目：HTTP/2 协议支持设置一个 TCP 连接上的最大并发流数目，从而限制其请求数目。
- DDOS攻击：分布式拒绝服务攻击，在多台机器一起攻击一个目标，通过大量互联网流量淹没目标或其周围基础设施，从而破坏目标服务器、服务或网络的正常流量时发生。

1.2 runC 漏洞对 UCS 服务的影响说明（CVE-2024-21626）

漏洞详情

runC是一个基于OCI标准实现的一个轻量级容器运行工具，是Docker、Containerd、Kubernetes等容器软件的核心基础组件。近日，runC社区发布最新版本，修复了一处高危级别的容器逃逸漏洞（**CVE-2024-21626**）。由于内部文件描述符泄漏，攻击者可通过控制容器进程的工作目录，或命令路径，将其设置为文件描述符的父级目录下的路径，读写主机任意文件，实现容器逃逸。

表 1-3 漏洞信息

漏洞名称	CVE-ID	漏洞级别	披露/发现时间
runC漏洞	**CVE-2024-21626**	高	2024-02-01

漏洞利用条件

UCS服务的正常使用场景不受此漏洞影响，仅当攻击者具备以下条件之一时，可利用该漏洞：

- 攻击者具有集群工作负载的创建或更新权限。
- 集群中工作负载的容器镜像来源不可信，攻击者拥有修改源镜像权限。

漏洞影响

满足上述漏洞利用条件时，容器进程可能逃逸到节点，导致节点信息泄露或执行恶意命令。

典型漏洞利用场景

- 攻击者具有集群工作负载的创建或更新权限，创建工作负载时设置容器进程的WORKDIR为/proc/self/fd/<num>，以实现在容器运行后访问节点文件系统。
- 工作负载的容器镜像来源不可信，攻击者拥有修改源镜像权限，将镜像中WORKDIR设置为/proc/self/fd/<num>，以实现在容器运行后访问节点文件系统。

判断方法

该漏洞范围涉及**中国站**本地集群和**国际站**多云集群类型，同时集群中工作负载配置或容器镜像具备如下特征时，可能存在风险：

- **工作负载中容器进程的WORKDIR为 /proc/self/fd/<num>。**

  图 1-1 有安全风险的工作负载配置示例

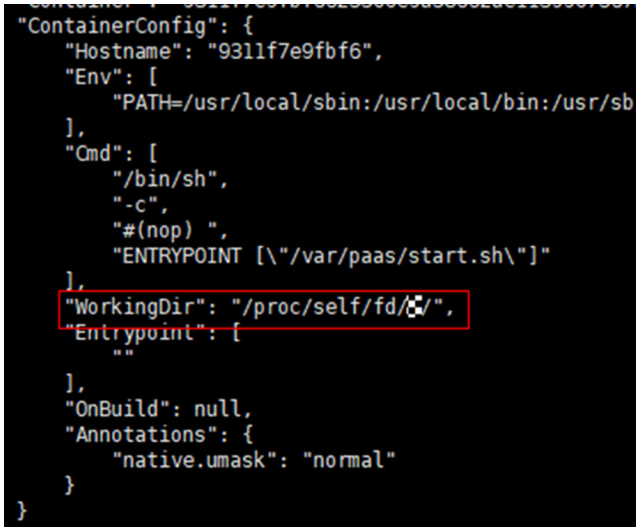
  ```
  spec:
    containers:
    - env:
      - name: PAAS_APP_NAME
        value: test-aatack-2
      - name: PAAS_NAMESPACE
        value: default
      image: nginx:latest
      imagePullPolicy: IfNotPresent
      name: container-1
      workingDir: /proc/self/fd/6
  ```

- **工作负载的容器镜像中默认WORKDIR或启动命令包含 /proc/self/fd/<num>。**

  可通过以下命令查看容器镜像元数据：

  - docker运行时执行：**docker inspect <镜像ID>**
  - containerd运行时执行：**crictl inspecti <镜像ID>**

图 1-2 有安全风险的工作负载配置示例



漏洞修复方案

规避措施

- 配置工作负载的WORKDIR为固定目录。
- 若未设置工作负载WORKDIR目录，需确保工作负载使用的容器镜像来源可信。

说明

执行以上规避措施前，请评估对业务的影响，并进行充分测试。

修复方案

当前UCS已修复该漏洞，请您使用最新版本的本地集群和多云集群。

参考链接

runC容器逃逸漏洞预警（CVE-2024-21626）

2 产品发布记录

2.1 集群联邦版本发布记录

表 2-1 UCS 集群联邦版本发布记录

UCS集群联邦版本号	支持的集群版本	更新特性	当前状态	UCS集群联邦版本商用时间	UCS集群联邦版本EOS（停止服务时间）
v1.10.7-r6	v1.19~v1.30	• 支持Kubernetes 1.30集群版本 • 支持MCI配置service维度的健康检查 • 支持MCI配置参数冲突校验	商用	2024.11	2026.11
v1.10.3-r10	v1.19~v1.29	修复集群状态异常时应用迁移问题	商用	2024.7	2026.7

2.2 组件版本发布记录

2.2.1 proxy-agent 组件版本发布记录

表 2-2 proxy-agent 组件版本发布记录

组件版本号	参数变更	变更时间	变更特性
proxy-agent:24.7.8.B001	无	2025.1	支持多通道隔离
proxy-agent:22.6.1	无	2022.6	无