云容器实例（CCI）

服务公告

文档版本 01

发布日期 2025-07-26

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 漏洞修复公告

1.1 修复 Linux 内核 SACK 漏洞公告

- 未关联ELB、EIP的容器实例，因为不对公网暴露，不受该漏洞影响，无需处理。
- 无状态负载（Deployment）：漏洞修复之后（7月11日0点之后）创建的无状态负载，不受该漏洞影响；漏洞修复之前（7月11日0点之前）创建的无状态负载，建议选择业务不受影响的时间窗口，**删除并重新创建负载的Pod实例**。
- 任务（Job）/定时任务（CronJob）：当前任务/定时任务执行完成后，下次任务/定时任务新建的Pod不再受该漏洞影响，无需处理。
- 插件：coredns插件不受该漏洞影响，无需处理。

漏洞详情

2019年6月18日，Redhat发布安全公告，Linux内核处理器TCP SACK模块存在3个安全漏洞(CVE-2019-11477、CVE-2019-11478、CVE-2019-11479)，这些漏洞与最大分段大小（MSS）和TCP选择性确认（SACK）功能相关，攻击者可远程发送特殊构造的攻击包造成拒绝服务攻击，导致服务器不可用或崩溃。

参考链接：

https://www.suse.com/support/kb/doc/?id=7023928

https://access.redhat.com/security/vulnerabilities/tcpsack

https://www.debian.org/lts/security/2019/dla-1823

https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SACKPanic?

https://lists.centos.org/pipermail/centos-announce/2019-June/023332.html

https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md

表 1-1 漏洞信息

漏洞类型	CVE-ID	披露/发现时间	华为云修复时间
输入验证错误	CVE-2019-11477	2019-06-17	2019-07-11
资源管理错误	CVE-2019-11478	2019-06-17	2019-07-11
资源管理错误	CVE-2019-11479	2019-06-17	2019-07-11

影响范围

影响Linux 内核2.6.29及以上版本。

解决方法

7月11日0点修复之前创建的无状态负载，建议选择业务不受影响的时间窗口，**删除并重新创建负载的Pod实例**。

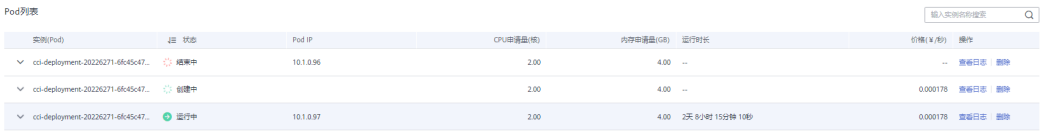
步骤1 登录云容器实例管理控制台，左侧导航栏中选择“工作负载 > 无状态（Deployment）”，单击负载名称。

步骤2 在无状态负载详情页面的Pod列表，单击Pod后的“删除”，在弹出的对话框中单击“是”。

图 1-1 删除相关 Pod

Pod删除后，Deployment会控制自动创建一个新的Pod，不需要您再进行新建，如图1-2所示。

图 1-2 自动创建 Pod



须知

存在多个Pod时，请逐个删除Pod，待前一个Pod重新创建成功后，再删除下一个Pod，避免业务发生中断。

----结束

附：TCP SACK 介绍

TCP是面向连接的协议。当双方希望通过TCP连接进行通信时，他们通过TCP握手交换某些信息建立连接，例如发起一个TCP请求，通过SYN发送初始序列ID、确认ID、连接使用的最大数据包段大小（MSS）、认证信息和处理选择性确认（SACK）等。整体TCP连接通过我们熟知的三次握手最终建立。

TCP通过一个数据段单元发送和接收用户数据包。 TCP数据段由TCP头、选项和用户数据组成。每个TCP段都有序列号（SEQ）和确认号（ACK）。

接收方通过SEQ号和ACK号来跟踪成功接收了哪些段。ACK号下一个预期接受的段。

示例：

上图中用户A通过13个100字节的段发送1k字节的数据，每个段具有20字节的TCP头，总计是13个段。在接收端，用户B接收了段1,2,4,6,8-13，而段3,5和7丢失，B没有接收到。

通过使用ACK号，用户B告诉A，他需要段3，用户A读取到B接收到2后没有收到3，A将重新发送全部段，尽管B已经收到了4,6和8-13段。这就导致了网络的低效使用。

1.2 kube-proxy 安全漏洞 CVE-2020-8558 公告

华为云CCI团队已经于7月10日识别kube-proxy安全漏洞CVE-2020-8558并对其进行了详细分析，分析结论为：**基于CCI服务当前形态，用户与CCI服务均不受本次漏洞的影响，无需进行处理**。

漏洞详情

Kubernetes官方发布安全漏洞（CVE-2020-8558），Kubernetes节点的设置允许相邻主机绕过本地主机边界进行访问。

Kubernetes集群节点上如果有绑定在127.0.0.1上的服务，则该服务可以被同一个LAN或二层网络上的主机访问，从而获取接口信息。如果绑定在端口上的服务没有设置身份验证，则会导致该服务容易受到攻击。

参考链接：

https://github.com/kubernetes/kubernetes/issues/92315

漏洞根因

kube-proxy为实现功能，开启了net.ipv4.conf.all.route_localnet=1内核参数。该参数允许内核接受来自其他节点的对于本机localhost的网络请求。

如何判断是否涉及漏洞

- 使用了受影响的集群版本
  - kubelet/kube-proxy v1.18.0-1.18.3
  - kubelet/kube-proxy v1.17.0-1.17.6
  - kubelet/kube-proxy <=1.16.10
- 集群内可信、不可信节点共享一个二层网络域（例如，同一个LAN）
- 集群允许不可信容器运行时包含CAP_NET_RAW（Kubernetes集群默认包含该能力）
- 节点（包含使用主机网络的容器）上存在监听localhost且未开启鉴权的服务

更多判断是否涉及漏洞的内容请参见**https://github.com/kubernetes/kubernetes/issues/92315**中“Am I vulnerable?”。

漏洞分析结果

综合以上分析，**CCI服务不受本次漏洞影响**，因为：

- CCI当前集群基于Kubernetes 1.15版本，但kube-proxy组件使用自研代码，不涉及net.ipv4.conf.all.route_localnet=1参数。
- CCI的集群形态与普通kubernetes集群不同。CCI基于安全容器并与华为云网络服务深度整合，用户VPC网络与CCI物理主机网络不在同一个2层域中。**CCI服务侧没有信息泄漏风险。**
- 用户容器内核默认没有开启net.ipv4.conf.all.route_localnet=1参数，用户绑定在localhost的进程无法进行同VPC内跨节点访问。**用户侧没有信息泄漏风险。**

1.3 CVE-2020-13401 的漏洞公告

华为云CCI团队已经于7月22日识别 Kubernetes 安全漏洞CVE-2020-13401并对其进行了详细分析，分析结论为：**用户与CCI服务均不受本次漏洞的影响，无需进行处理**。

漏洞详情

Kubernetes官方发布安全漏洞CVE-2020-13401，CVSS Rating: **CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L** (6.0 Medium)。

漏洞源于IPv6动态分配除提供了IPv6的DHCP技术外，还支持Router Advertisement技术。路由器会定期向节点通告网络状态，包括路由记录。客户端会通过NDP进行自身网络配置。

恶意攻击者可以篡改主机上其他容器或主机本身的IPv6路由记录，实现中间人攻击。即使现在系统或者服务上没有直接使用IPv6地址进行网络请求通知，但是如果DNS返回了A(IPv4)和AAAA(IPv6)记录，许多HTTP库都会尝试IPv6进行连接，如果再回退到IPv4，这为攻击者提供了响应的机会。

参考链接：**https://github.com/kubernetes/kubernetes/issues/91507**

如何判断是否涉及漏洞

Kubernetes本身不受该漏洞影响，但Kubernetes所使用的CNI插件（请参阅**containernetworking / plugins#484**）会受影响，以下kubelet版本都包含了受影响的CNI插件服务：

- kubelet v1.18.0~v1.18.3
- kubelet v1.17.0~v1.17.6
- kubelet<v1.16.11

漏洞分析结果

CCI服务不受本次漏洞影响，原因如下：

CCI当前集群基于Kubernetes 1.15版本，但未开启IPv6。所以**CCI节点没有被攻击的风险。**

1.4 CVE-2020-8559 的漏洞公告

华为云CCI团队已经于7月22日识别Kubernetes 安全漏洞CVE-2020-8559并对其进行了详细分析，分析结论为：**用户与CCI服务均不受本次漏洞的影响，无需进行处理**。

漏洞详情

近日Kubernetes官方披露了kube-apiserver组件的安全漏洞CVE-2020-8559，CVSS Rating: Medium (6.4) **CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H**。攻击者可以通过截取某些发送至节点kubelet的升级请求，通过请求中原有的访问凭据转发请求至其它目标节点，攻击者可利用该漏洞提升权限。

参考链接：**https://github.com/kubernetes/kubernetes/issues/92914**

如何判断是否涉及漏洞

使用了受影响的集群版本

- kube-apiserver v1.18.0-1.18.5
- kube-apiserver v1.17.0-1.17.8
- kube-apiserver v1.16.0-1.16.12
- all kube-apiserver versions prior to v1.16.0

漏洞分析结果

CCI服务不受本次漏洞影响，原因如下：

CCI当前集群基于Kubernetes 1.15版本，容器网络基于用户VPC，任何用户无法访问节点，也无法拦截kubelet请求。因此**节点没有被攻击的风险。**

1.5 CVE-2020-8557 的漏洞公告

华为云CCI团队已经于7月22日识别Kubernetes安全漏洞CVE-2020-8557并对其进行详细分析，分析结论为：**用户与CCI服务均不受本次漏洞的影响，无需进行处理**。

漏洞详情

Kubernetes官方发布安全漏洞CVE-2020-8557，CVSS Rating: Medium (5.5) **CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/CR:H/IR:H/AR:M**。

漏洞源于kubelet的驱逐管理器（eviction manager）中没有包含对Pod中挂载的/etc/hosts文件的临时存储占用量管理，因此在特定的攻击场景下，一个挂载了/etc/hosts的Pod可以通过对该文件的大量数据写入占满节点的存储空间，从而造成节点的拒绝访问（Denial of Service）。

参考链接：**https://github.com/kubernetes/kubernetes/issues/93032**

如何判断是否涉及漏洞

使用了受影响的集群版本：

- kubelet v1.18.0-1.18.5
- kubelet v1.17.0-1.17.8
- kubelet < v1.16.13

漏洞分析结果

CCI服务不受本次漏洞影响，原因如下：

- CCI当前集群基于 Kubernetes 1.15 版本，容器运行时选用 Kata 安全容器，节点上 hosts 文件并未直接挂载到容器内部。因此**节点没有被攻击的风险。**
- **不同租户的业务容器完全隔离，恶意用户无法影响其他用户。**

2 CCE 突发弹性引擎（对接 CCI）插件版本发布记录

CCE会定期发布CCE突发弹性引擎（对接CCI）插件新版本，进行特性更新、性能优化和BUG修复，以提升用户体验和系统稳定性。为了方便您能够体验最新功能、规避已知漏洞或问题，并保障业务的安全性和可靠性，建议定期升级至最新版本的CCE突发弹性引擎（对接CCI）插件。

表 2-1 CCE 突发弹性引擎（对接 CCI）插件版本记录

插件版本	支持的集群版本	更新特性
1.5.44	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29 v1.30 v1.31 v1.32	• 支持CCE v1.32集群 • 支持自动注入Sidecar容器 • 适配ARM64节点部署
1.5.29	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29 v1.30 v1.31	支持Pod配置指定子网

插件版本	支持的集群版本	更新特性
1.5.28	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29 v1.30 v1.31	功能优化
1.5.27	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29 v1.30 v1.31	支持CCE v1.31集群
1.5.26	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29 v1.30	问题修复
1.5.24	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29 v1.30	功能优化
1.5.16	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29 v1.30	仅进行Pod级别CPU和Memory资源规整

插件版本	支持的集群版本	更新特性
1.5.8	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29	适配CCE v1.29集群
1.3.57	v1.21 v1.23 v1.25 v1.27 v1.28	适配CCE v1.28集群
1.3.48	v1.21 v1.23 v1.25 v1.27	• 支持v1.25、v1.27版本集群 • 支持JuiceFS类型的存储
1.3.25	v1.17 v1.19 v1.21 v1.23	• 支持DownwardAPI Volume • 支持Projected Volume • 支持自定义StorageClass
1.3.19	v1.17 v1.19 v1.21 v1.23	支持schedule profile
1.3.7	v1.17 v1.19 v1.21 v1.23	支持v1.21、v1.23版本集群
1.2.12	v1.13 v1.15 v1.17 v1.19	• 新增了部分metrics指标 • 支持HPA与CustomedHPA • 支持将弹性到CCI的Pod中的hostPath转换为其它类型存储 • 修复Kubernetes Dashboard无法使用终端问题

插件版本	支持的集群版本	更新特性
1.2.5	v1.13 v1.15 v1.17 v1.19	• 自动清理CCI中不再被Pod依赖的资源 • 支持配置Requests与Limits不相等，弹性到CCI时的资源申请量以Limits为准 • 修复CCI命名空间不存在时插件卸载失败问题 • 增加对Pod规格超过CCI限制的创建请求的拦截
1.2.0	v1.13 v1.15 v1.17 v1.19	• 支持v1.19版本集群 • 支持SFS、SFS Turbo类型存储 • 支持CronJob • 支持配置envFrom • 日志文件自动转储 • 屏蔽TCPSocket类型健康检查 • 支持配置资源标签（pod-tag） • 提升了性能和可靠性 • 修复了一些已知问题
1.0.5	v1.13 v1.15 v1.17	支持v1.17版本集群