容器安全服务

最佳实践

文档版本 03

发布日期 2021-07-08

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。

目 录

1 容器入侵应急响应最佳实践

容器运行时安全功能对运行中的容器进行实时的逃逸检测、高危系统调用检测、异常进程检测、文件异常检测以及容器环境检测。在开启告警通知后，当CGS监测到异常事件时，您可收到CGS发送的告警通知邮件和短信。

本文介绍容器被入侵时和入侵后的应急响应。

背景信息

随着云原生的发展，容器使用场景越来越广泛，越来越多的企业选择容器来部署自己的应用。而针对容器的攻击事件频发，造成的破坏也日益严重。容器被入侵时，正常情况下黑客只能破坏容器自身，对其它容器和整个业务系统不容易造成整体的破坏。但是由于容器底层使用了共享操作系统内核、共享存储等技术方案，黑客有可能利用漏洞实现容器逃逸，进一步攻击主机操作系统，窃取数据、服务器受控等。因此，一旦确认容器被黑客成功入侵，需要立即处理，避免资产遭受重大损失。

前提条件

已确认CGS发送的告警信息为容器真实入侵告警信息。

容器入侵应急响应

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击 ☰，选择“安全与合规 > 容器安全服务”，进入“防护列表”界面。

步骤3 在左侧导航树中，选择“运行时安全”，进入“运行时安全”界面。

步骤4 获取入侵程序的容器实例名称和节点名称。

根据告警通知信息，选择不同页签（“逃逸检测”、“高危系统调用”、“异常程序检测”、“文件异常检测”、“容器环境检测”），在异常事件列表中，获取入侵程序的容器实例名称和节点名称。

图 1-1 异常事件列表

步骤5 断开容器外网链接。

以弹性负载均衡（ELB）为例，配置访问控制策略，允许特定IP访问，使其它IP不允许访问容器。

1. 在页面的左侧导航树中，单击 ☰，选择“网络 > 弹性负载均衡”，进入“负载均衡器”界面。
2. 找到容器使用的ELB实例。
3. 单击实例名称，进入详情页面，选择“监听器”页签。
4. 在监听器基本信息页面，单击“设置访问控制”。

图 1-2 设置访问控制

5. 在弹出的“设置访问控制”弹框中，配置白名单IP地址。
   - 访问策略：白名单。
   - IP地址组：允许特定IP访问的IP地址组。
   - 访问控制开关：开启。

图 1-3 配置白名单 IP 地址

6. 单击“确定”。

步骤6 中断目标容器运行。

以弹性云服务器控制台远程登录入侵节点为例，中断目标容器运行。

1. 在左侧导航树中，选择“弹性云服务器”，进入“弹性云服务器”界面。
2. 在**需要远程登录入侵节点**的操作列，单击“远程登录”，登录节点。
   若无法登录到服务器，请参见**无法登录到Linux云服务器怎么办**进行排查。

图 1-4 远程登录

3. 执行以下命令，获取目标容器ID号。
   docker ps|grep 容器实例名称
4. 执行以下命令，暂停挂起目标容器。
   docker pause 容器ID号

步骤7 保留入侵痕迹。

1. 执行以下命令，导出镜像。
   docker save ID号 -o 镜像文件名.tar
2. （可选）执行以下命令，导出配置。
   docker inspect ID号 > 配置文件名.json

步骤8 溯源分析。

1. 在其他节点上导入**步骤7.1**导出的镜像，并执行以下命令。
   docker load - 镜像文件名.tar
2. 使用导入的镜像启动新容器。
   启动执行命令：
   docker run -d -it --name 容器名称 镜像ID /bin/bash
3. 联系技术支持，进入容器查询系统日志、搜索恶意文件等定位入侵原因和制定应急决策。

----结束

2 runc 符号链接挂载与容器逃逸漏洞（CVE-2021-30465）最佳实践

背景信息

近日，华为云关注到业界有安全研究人员披露runc 符号链接挂载与容器逃逸漏洞（CVE-2021-30465），攻击者可通过创建恶意POD及container，利用符号链接以及条件竞争漏洞，可挂载宿主机目录至 container 中，最终可能会导致容器逃逸。目前漏洞细节、POC已公开，风险高。

华为云提醒使用runc的用户及时安排自检并做好安全加固。

漏洞编号

CVE-2021-30465

漏洞名称

runc符号链接挂载与容器逃逸漏洞

影响范围

- 影响版本：runc <= 1.0.0-rc94
- 安全版本：runc 1.0.0-rc95

官方解决方案

目前官方已在最新的版本中修复了该漏洞，请受影响的用户及时升级安全版本。

下载地址：**https://github.com/opencontainers/runc/releases**。

检测与解决方案

华为云容器安全服务（CGS）支持对该逃逸漏洞的预防与逃逸行为监测能力。

CGS实时监测容器集群节点中的容器运行状，并对异常事件进行告警和提供解决方案。

- **检测周期**

实时检测

- **检测原理**

  详细的检测原理，请参见：**运行时安全漏洞检测原理说明**。

- **查看检测详情**

  进入“运行时安全”界面，查看容器逃逸异常监控趋势图和异常事件列表，详情请参见**图2-1**，您还可以根据异常事件列表提供的解决方案处理异常事件。

  - 逃逸预防监测：选择“容器环境检测”页签查看详细信息。
  - 逃逸行为监测：选择“逃逸检测”页签查看详细信息。

图 2-1 运行时安全检测结果

A 修订记录

发布日期	修改说明
2021-07-08	第三次正式发布。 服务入口刷新。
2021-06-04	第二次正式发布。 新增**runc符号链接挂载与容器逃逸漏洞（CVE-2021-30465）最佳实践**。
2021-05-27	第一次正式发布。