runc符号链接挂载与容器逃逸漏洞

方正 2021-07-16 发表

漏洞相关信息

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

产品型号及版本： CloudOS E3106P02及5.0版本

漏洞描述

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，利用符号链接以及条件竞争漏洞，可挂载宿主机目录至容器中，最终可能会导致容器逃逸， 使攻击者能够访问宿主机的文件系统。目前漏洞细节、POC已公开，风险高。漏洞级别为严重

漏洞解决方案

该漏洞只能通过升级版本方式规避，目前E3106P02版本通过发布docker补丁版本解决，CloudOS5.0版本正在开发过程中