云平台CloudOS否使用TOA 组件而有被FakeToa工具利用的风险?

吕喜庆 2023-12-16 发表

问题描述

近日一位名为BeichenDream 的用户在 Github上发布一个FakeToa项目，包含利用 TOA (Tcp Option Address)伪 IP 地址，继而突破安全访问控制的-个测试工具。经测试，利用该工具，攻击者可以将真实 IP 伪造成白名单内的IP，重新进行TCP 协议的三次握手，插入TCP Option，继而可以访问原本受限的敏感网络资源(如通过安全组隔离的ECS、RDS、存储等)。

解决方法

云平台未安装使用此组件，故不涉及。