态势感知、综合日志审计平台是否涉及TOA漏洞

漏洞相关 张家豪 2023-12-22 发表

漏洞相关信息

漏洞编号： 不涉及

漏洞名称： 关于开展TOA风险排查的紧急通知

产品型号及版本： 态势感知CSAP、综合日志审计平台CSAP-SA

漏洞描述

关于开展TOA风险排查的紧急通知

一、基本情况

12月1日，名为BeichenDream的用户在Github上发布一个项目，包含利用TOA（Tcp Option Address）伪造IP地址，继而突破安全访问控制的一个测试工具。


伪造的风险预警

通知预警类-重要通知单（反馈类）

1、正文

时限要求： 115 H

各位领导、同事好，接上级部门通知：

攻击者可以通过篡改 TOA（TCP Option Address）伪造网络流量源 IP 地址，引发流量异常集中，造成业务中断，或欺骗网络边界防护设备，进而未授权访问网络，现将详细信息预警如下：

一、风险信息

TOA 是 TCP 协议头中的字段，主要用于流量转发设备标记源 IP 地址。TOA 通常应用在负载均衡、CDN、网络边界访问控制系统等具有流量转发功能的设备和系统上，上述设备和系统广泛部署在网络中。

攻击者可利用境外开源 FakeTOA 技术修改 TCP 头中的Options 字段，写入虚假 IP 地址实现伪造源 IP 目的。FakeTOA技术可引发负载均衡、CDN 等设备或系统误判，导致网络流量转发异常，如集中转发到特定目的IP地址上，可造成负载
过高引发业务中断。此外，FakeTOA 技术也可结合IP白名单机制，引发攻击者欺骗网络防火墙等网络边界设备或系统，导致网络访问安全限制失效，进而未授权访问内网等安全防护对象。

目前已发现部分型号负载均衡设备被 FakeTOA 技术突破的情况，相关攻击方法及代码在网上传播，网络安全风险增大。

二、工作要求

1、请各单位及时开展排查处置，梳理负载均衡、CDN、网络访问控制系统等使用 TOA 进行源地址识别的设备和系统，排查安全隐患，评估受 FakeTOA 影响范围和风险。若涉及本单位资产，请将受影响资产信息、加固完成情况、采取的加固措施填写至附件。

2、针对受影响资产，建议采取如下防护措施：

• 针对受影响设备和系统，通过校验 TCP 头中 Options 字段的真实性，或关闭 TOA 功能并更换其他标记、识别源地址的方式方法，及时消控安全风险。
• 对部署使用的第三方负载均衡、CDN、网络访问控制系统，组织设备生产厂商排查隐患评估风险，采取临时加固措施，推动厂商尽快提供补丁并升级修补。

3、如发生因该漏洞造成的重大网络安全事件，及时反馈集团SOC，谢谢。

2、附件

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）。

TOA(TCP Option Address)是基于四层协议（TCP）获取真实源 IP 的方法，本质是将源 IP 地址插入 TCP 协议的 Options 字段，然后进行网络请求，进而获取客户端的真实IP地址。

二、影响范围及风险分析

网络访问控制机制（ACL）是目前最常见的安全隔离措施， 一旦被突破可能带来严重影响及安全风险。

该问题影响到的平台：xxx平台。

该问题具体的影响： （蓝色是示例）

(1) 云服务商实现网络访问控制措施的产品（如暴露在互联网的网络产品、网络安全产品、依赖在线升级的产品等）是否受影响，如有则说明具体影响及风险。

(2) 云平台安全架构及安全防护体系是否受影响，如有则说明具体影响及风险。

(3) 云服务商人员身份鉴别及远程运维是否受影响，如有则说明具体影响及风险。

(4) 租户身份鉴别及远程运维是否受影响，如有则说明具体影响及风

险。

(5) 租户应用系统防护体系、数据安全是否受影响（如面对南北向攻击、东西项攻击），如有则说明具体影响及风险。

(6) 其他影响及风险分析。

三、下一步采取的安全控制措施及工作建议

(1) 临时安全控制措施

(2) 长期安全控制措施

针对该问题的分析及工作建议：

漏洞解决方案
不涉及该漏洞