运维审计A2000-G是否涉及Linux Kernel 远程代码执行漏洞（CVE-2022-42720）

漏洞相关 **戴航** 2022-10-25 发表

漏洞相关信息

漏洞编号： CVE-2022-42720

漏洞名称： Linux Kernel 远程代码执行漏洞

产品型号及版本： A2000-G

漏洞描述

漏洞描述：Linux Kernel 中存在一个远程代码执行漏洞，由于net/wireless/scan.c 中处理multi-BSSID 元素的bss_ref_get 函数存在use-after-free 缺陷，经过身份验证的远程攻击者通过注入WLAN 帧，最终可实现在目标系统上任意执行代码。

影响范围：5.1 <= Linux Kernel <= 5.19.x

目前官方已发布新版本修复了上述漏洞，请受影响的用户尽快升级至最新版本进行防护。 官方下载链接：https://www.kernel.org Linux 代码库已发布补丁，请相关用户尽快应用此补丁：https://git.kernel.org/pub/scm/linux/kernel/git/wireless/wireless.g it/commit/?id=0b7808818cb9df6680f98996b8e9a439fa7bcc2f

漏洞解决方案

运维审计不涉及该漏洞