Ubuntu 16.04 本地提权漏洞复现

漏洞简介

Twitter 上 Nikolenko 发推表示 ubuntu 最新版本存在一个本地提权漏洞，并且提供了 EXP 下载地址（http://cyseclabs.com/exploits/upstream44.c），该漏洞在老版本中已经完成修复，但是在 ubuntu16.04 版本依旧可以被利用。

影响范围

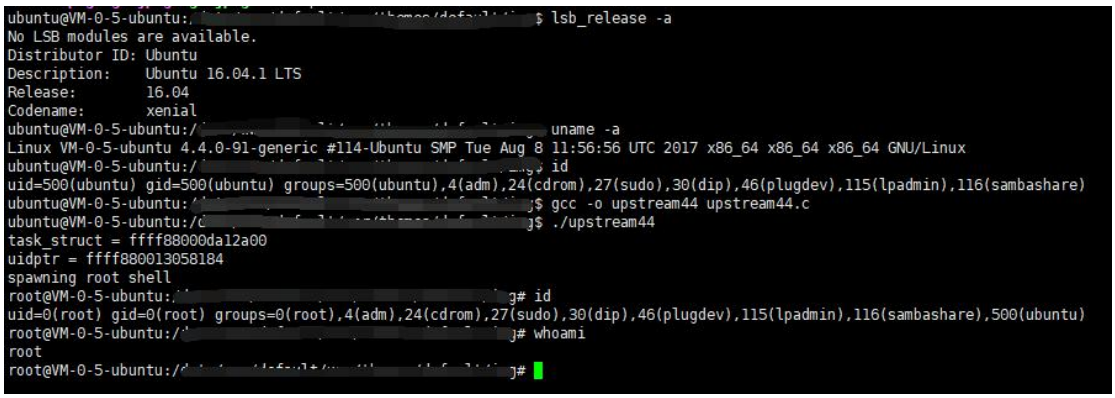
目前已知范围 ubuntu 16.04

复现环境

腾讯云 ubuntu 16.04.01

漏洞复现

使用在腾讯云平台上的主机测试，漏洞复现成功。



修复方案

目前暂未有明确的补丁升级方案。

建议用户在评估风险后，通过修改内核参数限制普通用户使用 bpf(2)系统调用：

echo 1 > /proc/sys/kernel/unprivileged_bpf_disabled

ubuntu 官网暂时没有提供修复方案，补丁更新请关注 ubuntu 官方漏洞公告：https://usn.ubuntu.com/