ADNET解决方案相关产品均不涉及Linux Kernel eBPF 权限提升漏洞

AD-NET解决方案 **路康** 2022-06-22 发表

漏洞相关信息

漏洞编号： CVE-2022-23222

漏洞名称： Linux Kernel eBPF 权限提升漏洞

产品型号及版本： 使用H3Linux1.1.2

漏洞描述

漏洞详情：

漏洞的存在是由于 Linux 内核的 BPF 验证器没有对 *_OR_NULL 指 针类型进行限制，允许这些类型进行指针运算。将一个 *_OR_NULL 类 型的 NULL 指针 r0 传递给 r1 ， 再将 r1 加 1 ， 然后对 r0 进行 NULL 检 查，此时 eBPF 会认为 r0 和 r1 都为 0 ， 但实际上 r0 为 0 r1 为 1 攻击者可以利用这个漏洞提升本地权限至 ROOT 。

影响版本： 5.8.0 <= Linux kernel <= 5.16

漏洞解决方案

ADNET相关涉及Linux操作系统的产品均使用H3Linux1.1.2及以下版本，其kernel内核版本为3.10，不涉及Linux Kernel eBPF 权限提升漏洞。

H3LINUX：H3Linux Release 1.1.2

KERNEL：kernel-3.10.0-957.27.2.el7.x86_64_03.tar.bz2