安全产品涉及漏洞编号CVE-2024-1086情况

漏洞相关 **孔梦龙** 2024-06-07 发表

漏洞相关信息

漏洞编号： CVE-2024-1086
漏洞名称： Linux内核被曝存在提取权限漏洞
产品型号及版本： 不区分

漏洞描述

关于Linux存在提权漏洞的风险提示

近日，Linux内核被曝存在提取权限漏洞 (漏洞编号CVE-2024-1086），攻击者利用该漏洞可在本地进行提权操作，最高可获取目标服务器的root管理权限。目前官方已经升级内核版本修复漏洞，请排查受漏洞影响情况，及时修复漏洞。
影响范围：
3.15<= Linux kernel < 6.1.76
5.2<= Linux kernel < 6.6.15
6.7<= Linux kernel < 6.7.3
6.8:rc1 = Linux kernel
该漏洞不适用于内核配置CONFIG_INIT_ON_ALLOC_DEFAULT_ON=y且Linux内核版本>6.4的Linux系统。
修复方案：
（1）升级Linux内核版本修复漏洞。
（2）若相关用户暂时无法进行更新，如果业务不需要，可以通过阻止加载受影响的 netfilter (nf_tables) 内核模块来缓解。
（3）如果无法禁用该模块，可在非容器化部署中，对用户命名空间进行限制。
响应处置要求:请排查受漏洞影响情况，及时修复漏洞。

漏洞解决方案

（1）安全V7产品不涉及
（2）

设备类型	是否涉及CVE-2024-1086漏洞
NS-SecPath AFC2100-D-G2	不涉及
NS-SecPath AFC2040-G2	不涉及
NS-SecPath A2025-G	不涉及
NS-SecPath A2025-G	不涉及
NS-SecPath D2015-G	不涉及
NS-SecPath SysScan-ME	不涉及
NS-SecPath SysScan-ME	不涉及
NS-SecPath W2020-G2	不涉及
NS-SecPath W2020-G2	不涉及
NS-SecPath ACG1000-AE	不涉及