SNA Center涉及Linux Netfilter本地权限提升漏洞

SNA Center 田毓磊 2021-07-24 发表

漏洞相关信息

漏洞编号： CVE-2021-22555
漏洞名称： Linux Netfilter本地权限提升漏洞
产品型号及版本： SNA Center E1209

漏洞描述

2021年07月16日，国外安全研究员Andy Nguyen公开了CVE-2021-22555 Linux Netfilter漏洞POC，该漏洞已在Linux内核代码中存在15年，攻击者成功利用此漏洞可以完成特权提升及实现docker、kubernetes环境逃逸。 建议受影响的用户将Linux Kernel升级到最新版本。

Netfilter是Linux 2.4.x引入的一个子系统，它作为一个通用的、抽象的框架，提供一整套的hook函数的管理机制，使得诸如数据包过滤、网络地址转换(NAT)和基于协议类型的连接跟踪成为了可能。

Linux是一种开源电脑操作系统内核。它是一个用C语言写成，符合POSIX标准的类Unix操作系统，一些组织或厂家，将Linux系统的内核与外围实用程序（Utilities）软件和文档包装起来，并提供一些系统安装界面和系统配置、设定与管理工具，就构成了一种Linux发行版本。

Linux 内核模块Netfilter中存在一处权限提升漏洞，攻击者可以通过漏洞实现权限提升，以及从docker、 kubernetes环境中逃逸。

这个操作一般只限于root用户，但是如果内核编译选项中启用了 CONFIG_USER_NS和CONFIG_NET_NS，并且赋予了普通用户高级特权，那么也能用于普通用户的进一步权限提升。

安全研究人员指出，该漏洞Crash信息最早曾在2020年8月17日由 syzbot公布在网上，不排除已被在野利用的可能。

漏洞解决方案

根据 RedHat 的建议，用户可以实施以下操作通过禁用非特权用户执行CLONE_NEWUSER、 CLONE_NEWNET，以缓解该漏洞带来的影响。

echo 0 > /proc/sys/user/max_user_namespaces