态势感知是否涉及CVE-2021-4034

漏洞相关 王树岭 2024-07-18 发表

漏洞相关信息

漏洞编号： CVE-2021-4034
漏洞名称： polkit
产品型号及版本： csap-s系列

漏洞描述

在 polkit 的 pkexec 程序中发现了一个本地权限提升漏洞。pkexec 应用程序是一个 setuid 工具，旨在允许非特权用户根据预定义的策略以特权用户身份运行命令。由于当前版本的 pkexec 无法正确处理调用参数计数，并最终会尝试将环境变量作为命令执行。攻击者可以通过控制环境变量，从而诱导 pkexec 执行任意代码。利用成功后，可导致非特权用户获得管理员权限。CVE-2021-4034

polkit 的 pkexec 存在本地权限提升漏洞，已获得普通权限的攻击者可通过此漏洞获取root权限。

目前漏洞POC已被泄露，攻击者利用该漏洞可导致恶意用户权限提升等危害

该漏洞CVSS评分：7.8

危害等级：高危

影响范围

2009年5月至今发布的所有 Polkit 版本

Polkit预装在CentOS、Ubuntu、Debian、Redhat、Fedora、Gentoo、Mageia等多个Linux发行版上，所有存在Polkit的Linux系统均受影响。
受影响版本
目前主流Linux版本均受影响。以下polkit版本为对应操作系统的修复版本：

1）CentOS系列：

CentOS 6：polkit-0.96-11.el6_10.2
CentOS 7：polkit-0.112-26.el7_9.1
CentOS 8.0：polkit-0.115-13.el8_5.1
CentOS 8.2：polkit-0.115-11.el8_2.2
CentOS 8.4：polkit-0.115-11.el8_4.2

2）Ubuntu系列：

Ubuntu 20.04 LTS：policykit-1 - 0.105-26ubuntu1.2
Ubuntu 18.04 LTS：policykit-1 - 0.105-20ubuntu0.18.04.6
Ubuntu 16.04 ESM：policykit-1 - 0.105-14.1ubuntu0.5+esm1
Ubuntu 14.04 ESM：policykit-1 - 0.105-4ubuntu3.14.04.6+esm1

3）BClinux 8.x

BClinux 8.6：policykit-0.115-13.an8.2.x86_64

目前各Linux发行版官方均已给出安全补丁，建议尽快升级至安全版本，如生产实际受限，我们可以采用官方提供的缓解措施来处理。如下：

https://ubuntu.com/security/CVE-2021-4034
https://access.redhat.com/security/cve/CVE-2021-4034
https://security-tracker.debian.org/tracker/CVE-2021-4034

漏洞解决方案

不涉及漏洞