KernelSU v0.5.7 Flaw Lets Android Apps Gain Root Access - Against Invac

Data: 2025-08-14 18:38:50

Autor: Inteligência Against Invaders

A vulnerability in KernelSU version 0.5.7 that could allow attackers to impersonate its manager

application and gain root access has been uncovered by cybersecurity researchers.

According to Zimperium's zLabs researchers, the flaw highlights ongoing weaknesses in rooting and jailbreaking frameworks, which are often built by independent developers without formal security oversight.

The team's analysis, published on Wednesday, shows how attackers could exploit design flaws in authentication to bypass safeguards.

KernelSU, along with tools like APatch and SKRoot, typically gains root access through Android kernel patching, hooking into key kernel functions to execute arbitrary code. This enables powerful management features, but also creates dangerous attack surfaces.

Rooting frameworks generally use one of two authentication methods:

- Password-based, where passwords can be weak or validation flawed, as seen in APatch and SKRoot
- Package-based, where the kernel trusts a manager app's package name or signature, as in KernelSU

KernelSU's package-based method relied on checking the first matching APK file in a process's file descriptor table. Attackers could manipulate file descriptor order to present the legitimate manager's APK first, bypassing signature checks.

Read more on Android security risks: Large-Scale Malicious App Campaign Bypassing Android Security

The exploit required the attacker's app to run before the legitimate manager, such as after a reboot, and could be triggered automatically by using the RECEIVE_BOOT_COMPLETED permission. While timing constraints limited the attack, it remained practical under realistic conditions.

Zimperium noted that similar vulnerabilities are widespread, with common issues including:

- Missing or weak authentication between user apps and kernel modules
- Overreliance on user-space input without validation
- Insecure communication channels
- Poor privilege isolation between apps and root-level functions

Past examples include an APatch flaw that allowed any app to run privileged operationsand Magisk’s CVE-2024-48336, which let local apps impersonate Google Mobile Services to silently gain root access.

The researchers concluded that nearly every rooting framework experiences critical vulnerabilities during its lifecycle, largely due to the complexity of modifying kernel behavior from user space and the absence of structured security reviews.