Samsung parandas KNOX-i kernelivea, mis ohustas Galaxy seadmeid

4 kuud tagasi - 24.06.2026 Autor: AM

Samsung parandas jaanuaris 2026 KNOX-i kernelivea, mis võis PROCA ja FIVE vahelise võidujooksu kaudu põhjustada mälukahjustuse ning mõjutada mitmeid Galaxy seadmeid, kirjutab Security Affairs.

Viga asus KNOX-i kaitsekihis

Turbeuurijad leidsid Samsungi KNOX-i *stack*'ist kernelitaseme *use-after-free* vea tähisega CVE-2026-20971. Viga paiknes PROCA ja FIVE vahelises koostoimes, kus süsteemid kontrollivad protsesside terviklikkust.

LucidBit Labsi raporti järgi tekkis probleem olukorras, kus protsess muutis olekut, näiteks *fork*'i või execve() kaudu. Sel hetkel vabastati vana *task_integrity* objekt ja asendati see uuega.

Rünnak sõltus ajastusest

Raporti järgi tekitas Androidi ennetav kernel väikese ajavahe, mida ründaja sai ära kasutada. Üks lõim võis pointeri lugeda, seejärel katkestuda ja hiljem kasutada juba vabastatud mälu.

LucidBit Labsi kirjelduses jooksis protsess *execve()* kaudu edasi, *task_integrity_put(old_tint)* vabastas algse struktuuri ning *proc_integrity_value_read()* jätkas kasutamist vabastatud mälule viitava *pointer* iga. Raporti hinnangul pidi protsess õigel hetkel ajaliselt välja langema.

Turvamehhanism ei takistanud väärkasutust

Samsungi KCFI vähendas küll ründe võimalusi, piirates suvaliste funktsioonikutsete kasutamist, kuid ei kõrvaldanud viga. Uurijad leidsid siiski tee, kasutades faili, mida ei saa käivitada, ehk *mitten-ELF* faili, et turvaviga uuesti ära kasutada.

See eemaldab *reset_file refcount*'i takistuse ning lubab vabastatud mälu uuesti kontrollitult kasutada. LucidBit Labsi kogemuse järgi muutus viga seejärel

reaalseks kernelimälu kahjustuse teeks.

Viga võis tulla tavalise äpi kaudu

Raporti järgi sai viga käivitada usaldamata rakendusest ning see võis viia kernelimälu kahjustuseni. Uurijad märkisid ka, et võimalikud olid mitu mälukahjustuse primitiivi, mis võisid viia seadme täieliku ülevõtmiseni.

Samsung parandas vea jaanuaris

Samsung parandas vea 2026. aasta jaanuari uuenduses. Mõjutatud olid Galaxy S9 kuni Galaxy S25 mudelid, samuti A-seeria seadmed ning Exynose ja Qualcommi platvormidel töötavad seadmed Androidi versioonides 13, 14, 15 ja 16.

Samsungi teatel oli probleemiks vale sisendikontroll *SecSettings*is enne SMR Jan-2026 Release 1 uuendust. Ettevõtte hinnangul oli ründe eelduseks kohalik ligipääs ja kasutaja sekkumine.

Raport rõhutas laiemaid riske

LucidBit Labsi raporti järgi ei ole kaitsev komponent kernelis automaatselt ohutu. Kui selline mehhanism kontrollib protsessi olekut või usaldusotsuseid, jääb see samuti ründepinnale.

Raport tõi ka välja, et töötajate seadmete kompromiteerimine võib anda ründajale lähtepunkti ettevõtte sisevõrku. Uurijate sõnul näitas juhtum ka seda, et kerneli CFI oli selles olukorras väga tõhus leevendus, kuigi muud tugevad primitiivid olid siiski olemas.

- Uudised
- Turvalisus

Pilt

