

Main Core (Assembly)

Null Filtering

1: call malloc ;return
pointer 0x12340000 in r1

2: mov r2, #8
; r2 is not a pointer

3a: mov r3, #1

3b: str r3, [r1, #12]
; store to 0x1234000c

4: add r2, r2, r3

1: rf_null[1] = false

2: rf_null[2] = true

3: rf_null[3] = true

3b: if (rf_null[1] && rf_null[3]) {
// drop monitoring
}
mem_null[r3 + 12] = rf_null[r3]

4: if (rf_null[2] && rf_null[3]) {
// drop monitoring
}
rf_null[r3] = rf_null[3] & rf_null[2]