

Analysis of the bug

The `do_addkey()` function doesn't set `keys[i]` to `NULL` after freeing an invalid key. This will cause a use-after-free in `do_grep()`.