

**Command used:** klee --simplify-sym-indices --write-cvcs --write-cov --output-module --max-memory=1000 --disable-inlining --optimize --use-forked-solver --use-cex-cache --libc=uclibc --posix-runtime --external-calls=all --only-output-states-covering-new --max-sym-array-size=4096 --max-solver-time=30s --max-time=1min --watchdog --max-memory-inhibit=false --max-static-fork-pct=1 --max-static-solve-pct=1 --max-static-cpfork-pct=1 --switch-type=internal --search=random-path --search=nurs:covnew --use-batching-search --batch-instructions=10000 ./paste.bc --sym-args 0 1 10 --sym-args 0 2 2 --sym-files 1 8 --sym-stdin 8 --sym-stdout

```
klee@cc46b0d750c1:~/coreutils-9.0/obj-llvm/src/klee-out-9$ cat test000001.ptr.err
Error: memory error: out of bound pointer
File: ./src/paste.c
Line: 208
assembly.ll line: 5202
State: 7
Stack:
#000005202 in paste_parallel(nfiles=3, fnamptr=94863350221688) at ./src/paste.c:208
#100004722 in __klee_posix_wrapped_main(argc=4, argv=94863350221680) at ./src/paste.c:520
#200002885 in __user_main(argcPtr=15, argvPtr=94863338833024, envp=94863338833152) at klee_src/runtime/POSIX/klee_init_env.c:245
#300000590 in __uClibc_main(15, 94863338833024) at libc/misc/internals/__uClibc_main.c:401
#400000756 in main(15, 94863338833024)

Info:
address: 94863350574016
next: object at 22724307597000 of size 4
MO268[4] (no allocation info)
klee@cc46b0d750c1:~/coreutils-9.0/obj-llvm/src/klee-out-9$ cat test000004.ptr.err
Error: memory error: out of bound pointer
File: ./src/paste.c
Line: 212
assembly.ll line: 5209
State: 27
Stack:
#000005209 in paste_parallel(nfiles=2, fnamptr=94863350221696) at ./src/paste.c:212
#100004722 in __klee_posix_wrapped_main(argc=4, argv=94863350221680) at ./src/paste.c:520
#200002885 in __user_main(argcPtr=15, argvPtr=94863338833024, envp=94863338833152) at klee_src/runtime/POSIX/klee_init_env.c:245
#300000590 in __uClibc_main(15, 94863338833024) at libc/misc/internals/__uClibc_main.c:401
#400000756 in main(15, 94863338833024)

Info:
address: 94863350380032
next: object at 22724307597000 of size 4
MO268[4] (no allocation info)
klee@cc46b0d750c1:~/coreutils-9.0/obj-llvm/src/klee-out-9$
```

## Error1 output as reported by KLEE

ktest file : 'test000001.ktest'  
args : ['./paste.bc', '--sym-args', '0', '1', '10', '--sym-args', '0', '2', '2', '--sym-files', '1', '8', '--sym-stdin', '8', '--sym-stdout']  
num objects: 11  
object 0: name: 'n\_args'









```
args : ['./paste.bc', '--sym-args', '0', '1', '10', '--sym-args', '0', '2', '2', '--sym-files', '1', '8',
'--sym-stdin', '8', '--sym-stdout']
num objects: 11
object 0: name: 'n_args'
object 0: size: 4
object 0: data: b'\x01\x00\x00\x00'
object 0: hex : 0x01000000
object 0: int : 1
object 0: uint: 1
object 0: text: ....
object 1: name: 'arg00'
object 1: size: 11
object 1: data: b'--\x00\xff\xff\xff\xff\xff\xff\xff\xff'
object 1: hex : 0x2d2d00ffffffffffff
object 1: text: --.....
object 2: name: 'n_args'
object 2: size: 4
object 2: data: b'\x02\x00\x00\x00'
object 2: hex : 0x02000000
object 2: int : 2
object 2: uint: 2
object 2: text: ....
object 3: name: 'arg01'
object 3: size: 3
object 3: data: b'\xff'
object 3: hex : 0x2d2fff
object 3: text: -/.
object 4: name: 'arg02'
object 4: size: 3
object 4: data: b'\x00\x00\x00'
object 4: hex : 0x000000
object 4: text: ...
object 5: name: 'A_data'
object 5: size: 8
object 5: data: b'\x00\x00\x00\x00\x00\x00\x00\x00'
object 5: hex : 0x0000000000000000
object 5: int : 0
object 5: uint: 0
object 5: text: .....
object 6: name: 'A_data_stat'
```









