It turns out that memcpy(NULL, _, 0) is undefined behaviour (sigh), and that this can actually matter. This article has a good explanation.

Legal usage of specvec -- copying a zero-length vector -- can invoke this.

I noticed this when starting a server compiled with UBSan (gcc -fsanitize=undefined):

```
2: Loading rulesets.
/home/jtn/src/freeciv/git26/utility/specvec.h:117:3: runtime error: null pointer passed as argument 1, which is declared to never be null
 #0 0x556be4152a18 in requiremment_vector_copy /home/jtn/src/freeciv/git26/utility/specvec.h:117
 #1 0x556be4188303 in load_ruleset_cities /home/jtn/src/freeciv/git26/server/ruleset.c:4820
 #2 0x556be41a5f6d in load_rulesetdir /home/jtn/src/freeciv/git26/server/ruleset.c:7067
 #3 0x556be41a5a44 in load_rulesets /home/jtn/src/freeciv/git26/server/ruleset.c:6938
 #4 0x556be3e95c37 in srv_prepare /home/jtn/src/freeciv/git26/server/srv_main.c:2939
 #5 0x556be3e999f55 in srv_main /home/jtn/src/freeciv/git26/server/srv_main.c:3342
 #6 0x556be3e720d3 in main /home/jtn/src/freeciv/git26/server/civserver.c:476
 #7 0x7f303298a09a in __libc_start_main ../csu/libc-start.c:308
 #8 0x556be3e6f1e9 in _start (/home/jtn/src/freeciv/git26/build-asan/server/freeciv-server+0xe331e9)
2: AI*1 has been added as Easy level AI-controlled player (classic).
```

(This is setting up the specialist reqs vectors, which are all empty in the 2.6 default ruleset.)

I've no evidence that this actually caused a user-visible bug with common toolchains.

I haven't gone out of my way to audit for other instances.

---

**History**

**#1 - 2020-03-07 04:21 PM - Jacob Nevins**

- File m-30-26-specvec-ub.patch added
- Status changed from In Progress to Resolved

**#2 - 2020-03-08 02:30 PM - Chippo Elder**

I used S3_0, clang and UBSan and replicated the warning:

```
2: Loading rulesets.
../utility/specvec.h:117:10: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/string.h:43:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../utility/specvec.h:117:10 in
../utility/specvec.h:117:17: runtime error: null pointer passed as argument 2, which is declared to never be null
/usr/include/string.h:43:28: note: nonnull attribute specified here
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../utility/specvec.h:117:17 in
```

The patch didn't apply, though it looks fine to me:
chippo@chippo-Aspire-V3-731:~/Downloads/git_clones/freeciv/freeciv-30$ git apply ../m-30-26-specvec-ub.patch
error: specvec.h: No such file or directory

So, I applied it with vi

chippo@chippo-Aspire-V3-731:~/Downloads/git_clones/freeciv/freeciv-30$ git diff
diff --git a/utility/specvec.h b/utility/specvec.h
index 22627d07eb..7102873396 100644
--- a/utility/specvec.h
+++ b/utility/specvec.h
@@ -114,7 +114,9 @@ static inline void SPECVEC_FOO(_vector_copy) (SPECVEC_VECTOR *to,
 const SPECVEC_VECTOR *from)
 {
     SPECVEC_FOO(_vector_reserve) (to, from->size);
-    memcpy(to->p, from->p, from->size * sizeof(*to->p));
+    if (from->size > 0) {
+        memcpy(to->p, from->p, from->size * sizeof(*to->p));
+    }
 }

static inline void SPECVEC_FOO(_vector_free) (SPECVEC_VECTOR *tthis)

and can confirm that it takes the warnings away for llvm UBSan and S3.0.

#3 - 2020-03-09 08:00 AM - Jacob Nevins
- Status changed from Resolved to Closed

Files

m-30-26-specvec-ub.patch  928 Bytes  2020-03-07  Jacob Nevins