```
**********************************************************
   10668 Tue Jan 13 19:02:47 2015
new/usr/src/cmd/sgs/libelf/common/clscook.c
5535 libelf should check for e_phoff overflow
**********************************************************
______unchanged_portion_omitted_
```

```
295 int
296 _elf_phdr(Elf * elf, int inplace)
297 {
298         NOTE(ASSUMING_PROTECTED(*elf))
299         register size_t         fsz, msz;
300         Elf_Data                dst, src;
301         Ehdr *                  eh = elf->ed_ehdr;      /* must be present */
302         unsigned                work;

304         if (eh->e_phnum == 0)
305                 return (0);

307         fsz = elf_fsize(ELF_T_PHDR, 1, elf->ed_version);
308         if (eh->e_phentsize != fsz) {
309                 _elf_seterr(EFMT_PHDRSZ, 0);
310                 return (-1);
311         }

313         fsz *= eh->e_phnum;
314         ELFACCESSDATA(work, _elf_work)
315         msz = _elf_msize(ELF_T_PHDR, work) * eh->e_phnum;
316         if ((eh->e_phoff == 0) ||
317             (elf->ed_fsz <= eh->e_phoff) ||
318             (elf->ed_fsz - eh->e_phoff < fsz)) {
317             ((fsz + eh->e_phoff) > elf->ed_fsz)) {
319                 _elf_seterr(EFMT_PHTAB, 0);
320                 return (-1);
321         }

323         if (inplace && fsz >= msz && eh->e_phoff % sizeof (ElfField) == 0) {
324                 elf->ed_phdr = (Elf_Void *)(elf->ed_ident + eh->e_phoff);
325                 elf->ed_status = ES_COOKED;
326         } else {
327                 if ((elf->ed_phdr = malloc(msz)) == 0) {
328                         _elf_seterr(EMEM_PHDR, errno);
329                         return (-1);
330                 }
331                 elf->ed_myflags |= EDF_PHALLOC;
332         }
333         src.d_buf = (Elf_Void *)(elf->ed_ident + eh->e_phoff);
334         src.d_type = ELF_T_PHDR;
335         src.d_size = fsz;
336         src.d_version = elf->ed_version;
337         dst.d_buf = elf->ed_phdr;
338         dst.d_size = msz;
339         dst.d_version = work;
340         if ((_elf_vm(elf, (size_t)eh->e_phoff, fsz) != OK_YES) ||
341             (elf_xlatetom(&dst, &src, elf->ed_encode) == 0)) {
342                 if (elf->ed_myflags & EDF_PHALLOC) {
343                         elf->ed_myflags &= ~EDF_PHALLOC;
344                         free(elf->ed_phdr);
345                 }
346                 elf->ed_phdr = 0;
347                 return (-1);
348         }
349         elf->ed_phdrsz = msz;
350         return (0);
```



```
351 }
______unchanged_portion_omitted_
```