New issue

Jump to bottom

There is a buffer overflow when parsing command line parameters #294

Open **firmianay** opened this issue on Jul 23, 2021 · 1 comment

firmianay commented on Jul 23, 2021 • edited

Hi friends!
When the parameter length is greater than 100 characters of MAX_CHAR, the strcpy function overflows. A length check can be performed to fix the problem.

```
  #define MAX_CHAR (100)

          char umfile[MAX_CHAR];
          char navfile[MAX_CHAR];
          char outfile[MAX_CHAR];



          while ((result=getopt(argc,argv,"e:u:g:c:l:o:s:b:T:t:d:iv"))!=-1)
          {
                  switch (result)
                  {
                  case 'e':
                          strcpy(navfile, optarg);
                          break;
                  case 'u':
                          strcpy(umfile, optarg);
                          nmeaGGA = FALSE;
                          break;
                  case 'g':
                          strcpy(umfile, optarg);
                          nmeaGGA = TRUE;
                          break;
                  case 'c':
                          // Static ECEF coordinates input mode
                          staticLocationMode = TRUE;
                          sscanf(optarg,"%lf,%lf,%lf",&xyz[0][0],&xyz[0][1],&xyz[0][2]);
                          break;
                  case 'l':
                          // Static geodetic coordinates input mode
                          // Added by scateu@gmail.com
                          staticLocationMode = TRUE;
                          sscanf(optarg,"%lf,%lf,%lf",&llh[0],&llh[1],&llh[2]);
                          llh[0] = llh[0] / R2D; // convert to RAD
                          llh[1] = llh[1] / R2D; // convert to RAD
                          llh2xyz(llh,xyz[0]); // Convert llh to xyz
                          break;
                  case 'o':
                          strcpy(outfile, optarg);
                          break;
```

firmianay commented on Jun 30 • edited   Author

https://nvd.nist.gov/vuln/detail/CVE-2021-37778
Discoverer: Chao Yang@CAERI

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant