Document: N1562

Submitter: Martin Sebor, Robert Seacord
Submission Date: 2011-03-10
Source:
Reference Document:
Version:
Date: 2011-03-10
Subject: putc() and getc() macros

The C99 standard specifies that the getc(), putc(), getwc(), and putwc() functions may be implemented as macros that evaluate their stream argument more than once, and discourages programs from invoking the functions (or macros) with an argument that has side effects.

To minimize the risk of security related defects due to this error the CERT C Secure Coding Standard requires that conforming programs avoid calling getc() or putc() with arguments that have side effects.
See:

> FIO41-CPP. Do not call getc() or putc() with stream arguments that have side effects
> http://www.securecoding.cert.org/confluence/x/zoEyAQ

Adopting such a rule in an organization with thousands of engineers has non-trivial costs that could easily be avoided if the C1X standard were to remove the license for implementers to define the macros in this way.

The reason why the standad permits conforming implementations to define the functions as macros is efficiency. This reason has been largely obviated with the introduction of inline functions. In addition, an alternative technique exists that makes it possible to define the macros in a way that guarantees that each of their arguments is evaluated exactly once. The following example shows the Solaris definition of putc() as a macro using the GCC extension that guarantees that the stream argument is evaluated excactlty once:

```
#define putc(x, p) __extension__(({                    \
    FILE *__p = p;                                     \
    (  --(__p)->_cnt<  0                               \
     ? __flsbuf((x), (__p))                            \
     : (int)(*(__p)->_ptr++ = (unsigned char)(x)));    \
 }))
```

Suggested Technical Corrigendum

To improve the safety and security of C programs and reduce the cost of using language correctly we suggest to remove the implementation license to evaluate the stream argument more than once.

Specifically, we suggest to trike from the specification of functions getc(), putc(), getwc(), and putwc() the following text:

> , except that if it is implemented as a macro, it may evaluate stream more than once, so that argument should never be an expression with side effects.

The corrected description of each of the functions is below.

> 7.21.7.5 The getc function
>
> Description
> -2- The getc function is equivalent to fgetc.

> 7.21.7.7 The putc function
>
> Description
> -2- The putc function is equivalent to fputc.

> 7.28.3.6 The getwc function
>
> Description
> -2- The getwc function is equivalent to fgetwc.

> 7.28.3.8 The putwc function
>
> Description
> -2- The putwc function is equivalent to fputwc.