N2006

ISO/IEC 17961: Potential defect report and proposed change for C2X
Re: Rule 5.40: Using a tainted value to write to an object using a formatted input or output function

Introduction

These two suggestion have come from MISRA, as they are adding support for 17961 to their rules.

1) Potential defect report

Rule 5.40 names a number of functions that can attempt to write beyond the bounds of the target array, if supplied with tainted input, namely: fscanf, scanf, vfscanf, vscanf, sscanf, vsscanf and sprint

The observation is that vsprintf should be included in this list. Also the _s versions of all the above (including vsprintf_s) should be included, as they also can write beyond the end of the target array.

It is suggested that this is a defect rather than an enhancement, as from the rationale for the rule, they should have been included when drafted.

2) Proposed change for C2X

The following functions potentially have the same behaviour as the above: snprintf, vsnprintf, snprintf_s and vsnprintf_s, if the size parameter doesn't match the size of the target array.

It is proposed that the above four function are added to 5.40, with the additional constraint: 'It shall be diagnosed if the target array (s) is smaller than the indicated size (n)'

As this is an extension of the scope of the rule, it is suggested as an enhancement rather than a defect.