ISO/IEC JTC 1/SC 22/WG 23 N 0300

Proposed changes to WXQ and YZS re "volatile"

Date	14 December 2010
Contributed by	Tom Plum
Original file name	Email dated 14 December 2010
Notes	

Moore, Jim

From: Thomas Plum [tplum@plumhall.com]
Sent: Tuesday, December 14, 2010 5:20 PM
To: Moore, Jim; John Benito
Cc: Thomas Plum
Subject: WXQ and YZS, re "volatile"

[existing]

6.18 Dead Store [WXQ]
6.18.1 Description of application vulnerability
A variable's value is assigned but never subsequently used,
either because the variable is not referenced again, or
because a second value is assigned before the first is
used. This may suggest that the design has been
incompletely or inaccurately implemented, i.e. a value has
been created and then 'forgotten about'.

[proposed additional paragraph]

In C and C++, a _volatile_ variable is always assumed
to be "subsequently used", because storing to such variables
may have side effects unknown to the implementation.

[existing]

6.19 Unused Variable [YZS]
6.19.1 Description of application vulnerability
A variable is declared but neither read nor written in
the program, making it an unused variable. This type of error
suggests that the design has been incompletely or
inaccurately implemented.
Unused variables by themselves are innocuous, but can
combine with other vulnerabilities such as index bounds
errors or buffer overflows to mask errors or provide
hidden channels.

[no corresponding change is needed in YZS, because
"neither read nor written" applies equally to
volatile and non-volatile variables]

--+
Thomas Plum, Plum Hall Inc, 3 Waihona Box 44610, Kamuela HI 96743 USA
tplum@plumhall.com ..... TEL +1-808-882-1255 FAX +1-808-882-1556
http://www.PlumHall.com ..... TOLLFREE +1-800-PLUM-HALL (800-758-6425)