

## Exiv2 - Bug #1019

### Cppcheck: Suspicious usage of 'sizeof' with a numeric constant as parameter.

05 Jan 2015 21:14 - Thomas Beutlich

<b>Status:</b>	Closed	<b>Start date:</b>	05 Jan 2015
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Robin Mills	<b>% Done:</b>	100%
<b>Category:</b>	coverity	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>	0.25		
<b>Description</b>			
In jp2image.cpp lines 555, 561 and 567 there is sizeof(16) as third argument for memcmp. Cppcheck reports			
<pre>It is unusual to use a constant value with sizeof. For example, 'sizeof(10)' returns 4 (in 32-bit systems) or 8 (in 64-bit systems) instead of 10. 'sizeof('A')' and 'sizeof(char)' can return different results.</pre>			

#### Associated revisions

##### Revision 3538 - 08 Jan 2015 12:44 - Robin Mills

#1019. Thank You Thomas for finding this issue.

##### Revision 3547 - 09 Jan 2015 10:25 - Robin Mills

#1019. Thanks to private email with Thomas about the MSVC issue. Changed a signature in the patch to calm the compiler. MSVC is more strongly insistent than GCC or Clang about signature match.

#### History

##### #1 - 06 Jan 2015 12:44 - Robin Mills

- Category set to coverity
- Status changed from New to Assigned
- Assignee set to Robin Mills
- Target version set to 0.25

##### #2 - 08 Jan 2015 12:50 - Robin Mills

This is very suspicious! I think the sizeof(16) should simply be 16. It appears to be copying UUIDs which are 128 bits = 16 x 8bit bytes. The sizeof(16) would have "throttled" the UUID to 4 or 8 bytes. This would cause part of the data to be in an undefined state, without overflowing the buffer to which the data is being copied.

Fix submitted [r3538](#). Thank you Thomas for finding and reporting this.

##### #3 - 08 Jan 2015 12:50 - Robin Mills

- Status changed from Assigned to Resolved

##### #4 - 08 May 2015 16:33 - Robin Mills

- % Done changed from 0 to 100

##### #5 - 21 Jun 2015 16:39 - Andreas Huggel

- Status changed from Resolved to Closed