

## Exiv2 - Bug #447

### Buffer overflow in sscanf

09 Dec 2005 07:08 - Andreas Huggel

<b>Status:</b>	Closed	<b>Start date:</b>	
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Andreas Huggel	<b>% Done:</b>	0%
<b>Category:</b>	miscellaneous	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>	0.9		
<b>Description</b>			
sscanf expects a 0 terminated C-string to read from. In exiv2 the function is in some places called with a data buffer (not 0 terminated) instead. This causes a buffer overflow and may crash the application.			

### History

#1 - 10 Dec 2005 02:37 - Andreas Huggel

[r656](#)