Exiv2 - Bug #447
Buffer overflow in sscanf

09 Dec 2005 07:08 - Andreas Huggel

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Andreas Huggel	**% Done:**	0%
Category:	miscellaneous	**Estimated time:**	0.00 hour
Target version:	0.9		

Description

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