QGIS Application - Bug report #7371
QgsProject.writeEntry() makes it very easy to make a project file unreadable

2013-03-16 01:05 PM - Olivier Dalang

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	Project Loading/Saving		
Affected QGIS version:	master	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	Yes	**Resolution:**	fixed/implemented
Crashes QGIS or corrupts data:	No	**Copied to github as #:**	16344

Description

Hi !

When using QgsProject.instance().writeEntry(scope, key, value), it's really easy to make the whole project file unreadable.

This happens because scope and keys are used as XML elements names in the project file.

In case a plugin developer uses user input as the key, he may not notice that he's endangering the user's files.

I'd suggest to sanitize scope and keys to make sure the project's XML remains valid whatever scope/key is used.

I'm providing a patch which **is not finished**.
Here are the regexp that should be used for sanitation : http://www.w3.org/TR/REC-xml/#NT-NameStartChar
But I didn't manage to make that work, so the patch provides a much simpler regexp which is too restrictive (refuses foreign characters for instance).

Thanks !

Olivier

History

#1 - 2013-03-16 02:18 PM - Olivier Dalang

- % Done changed from 50 to 100

Ok I think I found the right regexp !

So I made a pull request : https://github.com/qgis/Quantum-GIS/pull/469

#2 - 2014-06-21 04:09 AM - Jürgen Fischer

- Category set to Project Loading/Saving

#3 - 2016-10-10 04:36 PM - Nyall Dawson

- Resolution set to fixed/implemented

- Status changed from Open to Closed

Fixed in commit:313fe6a98f06cc4094ace211fc3a191aa0497cd6

Files

0001-Implements-sanitation-of-entries-names.patch	2.43 KB	2013-03-16	Olivier Dalang