# Movian - Bug #2979
# German "Umlaute" probably generate a buffer overflow / corruption during JSON Encoding for storage

01/20/2016 01:25 PM - Christopher Skerra

| | | | |
|---|---|---|---|
| **Status:** | Fixed | **Start date:** | 01/20/2016 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Andreas Smas | **% Done:** | 100% |
| **Category:** | API | **Estimated time:** | 0.00 hour |
| **Target version:** | 4.10 | | |
| **Found in version:** | Movian 4.10.35.g83bb6 | **Platform:** | PS3 |

**Description**

I had a problem that in my plugin, the favorite list got deleted / new generated almost each time the user restarts movian.
After some hours of trying to reproduce the problem (cause it really did not happen each time) I came to this situation:
The code for createstore is called and then the check for store.favorites existence is done. This existence check failed and therefor generated a new list store.favorites = "[]";.
The reason for this was, after some try catching, that the JSON seemed to get corrupted and missed some ending: ]"}
Funny thing here: the number of missing closing symbols varied. sometimes only the } was missing.
And now on to the reason:
When the user tries to add an entry with an Umlaut like Flöte, the json encoding created FlÃ–te. And heres the problem:
The ö is converted to 2 characters Ã–. If we have more Umlauts, the problem gets even worse and we have multiple 1 to 2 character conversion.
This results in a problem for the write back to file call for the storage file (it seems).
For me it seems that the write back call uses the original length of the string
for example: {"favorites":"[{"test":"flöte"}]"}
but will write back{"favorites":"[{"test":"flÃ–te"}]"
-> see the missing }

I dont know if this is something the plugin developer should take care of or if the JSON Encoding / write back call needs some fix. One thing is for sure: That was a tough one to nail down -.-.

## Associated revisions

**Revision 242686b1 - 01/22/2016 04:03 PM - Andreas Smas**

ecmascript: Make native fs write code figure out length on its own

Fixes #2979

**Revision 41bb3aae - 01/22/2016 04:04 PM - Andreas Smas**

ecmascript: Make native fs write code figure out length on its own

Fixes #2979

## History

**#1 - 01/21/2016 09:35 AM - Andreas Smas**

*- Status changed from New to Accepted*

*- Target version set to 4.10*

Good catch and analysis. I know now where the problem is and i'll try to fix it later today.

Thanks!

**#2 - 01/22/2016 04:04 PM - Andreas Smas**

*- Status changed from Accepted to Fixed*

*- % Done changed from 0 to 100*

Applied in changeset commit:git|242686b1d8420446997af17812f16b88e0422e32.