**Issue Details** (XML)

**Key:** FP-1265
**Type:** Bug
**Status:** Community
**Priority:** None
**Assignee:** Charles Liss
**Reporter:** Sean Barrett
**Votes:** 0
**Watchers:** 0

**Flash Player**

# avm2 getlex crashes with abnormal scope stack and incorrect namespace

Created: 12/31/08 03:53 PM Updated: 12/31/08 05:02 PM

**Component/s:** ActionScript Runtime Errors

**Security Level:** Public (All JIRA Users )

**File Attachments:** 1. crash_1.swf (0.4 kb)

**Severity:** Crash/Hang

**Reproducibility:** Every Time

**Found in Version:** Flash Player 9 - 9_0_115_0

**Affected OS(s):** Windows - XP

**Steps to Reproduce:**

Steps to reproduce: « Hide
1. run attached crash_1.swf in flash player
2.
3.

Actual Results:
Crash

Expected Results:
Should run then produce an error since MainTimeline is not defined.

Additional comments:
The error was created while assembling AVM2 code directly, rather than through Flash CS, using the following as the constructor for the script defining MainTimeline:

```
pushbyte 0
pushscope
getlex ::Sprite // this is a notation for the public namespace, but something like foo::Object also crashes
returnvoid
```

Note that the "pushbyte 0 / pushscope" deviates entirely from normal CS-generated code, since it pushes something irrelevant on the scope stack, but

that irrelevant data is normally harmless; for example, the following works as expected:

```
pushbyte 0
pushscope
getlex flash.display::Sprite
construct 0
returnvoid
```

Crash occurs in both FlashPlayer 9 and 10.

I have not tested whether this bug occurs with getlex even after initialization, nor whether findproperty/findpropstrict/getproperty have similar issues.

| | |
|---|---|
| **Language Found:** | English |
| **Bugbase Id:** | none |
| **Participants:** | Charles Liss and Sean Barrett |
| **Browser:** | Firefox 2.x |

**All Comments** Sort Order:

Sean Barrett - [12/31/08 05:02 PM ] [ Permlink | « Hide ]

Further testing suggest the error occurs when running 'findproperty' with any undefined qname, e.g.:

```
pushbyte 0
pushscope
findproperty ::crap
returnvoid
```