Prelude-LML - Bug #226

prelude-lml segfault on rule error

05/18/2007 11:48 AM -

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Yoann VANDOORSELAERE	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.9.10		
Resolution:	fixed		

Description

I have the following rule in prelude-lml:

```
regex=message received; \
        add_context=MESSAGE_RECEIVED; \
        silent; \
        last;

regex=IP = (\S+); \
        require_context=MESSAGE_RECEIVED; \
        source(0).node.address(>>).address = $1; \
        last;
```

Now I add the following message to the log file I'm monitoring:

```
message received
IP = 1.2.3.4
```

This results in a segfault of prelude-lml:

```
- /tmp/test.log: Metadata available, starting log analyzis at offset 18341.
prelude-lml.c:lml_dispatch_log:225: [LOG] message received
could not match prefix against log entry: message received.
pcre-mod.c:pcre_context_new:998: [MESSAGE_RECEIVED]: creating context (expire=60s).
prelude-lml.c:lml_dispatch_log:225: [LOG] IP = 1.2.3.4
could not match prefix against log entry: IP = 1.2.3.4.
Segmentation fault
```

The rule works as expected when I change source(0).node.address(>>).address to source(>>).node.address(>>).address.

My version:

```
[root@blah ~]# prelude-lml --version
prelude-lml-0.9.9
```

History

#1 - 05/18/2007 05:37 PM - Yoann VANDOORSELAERE

- Status changed from New to Assigned

#2 - 05/19/2007 01:03 PM - Yoann VANDOORSELAERE

- Status changed from Assigned to Closed

- Resolution set to fixed

(In r9483) Fix NULL pointer dereference when a rule reference an existing, but empty context (fix #226).

#3 - 04/29/2009 12:21 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude-LML

- Category deleted (4)

- Target version deleted (0.9.10)