Prelude-LML - Bug #185

defective squid rule in prelude-lml

12/13/2006 09:41 PM - prmarino1-gmail-com -

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Yoann VANDOORSELAERE	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.9.8		
Resolution:	fixed		

Description

I found a defective rule in the squid.rules file
it has an error plus a missleading classification text and impact description
here is a sample of the log

```
r11323: Squid Parent: child process 10216 exited due to signal 6
```

here is what the rule currently is:

```
# No log sample; please submit
regex=Squid Parent: child process (\d+) exited; \
 classification.text=Proxy stopped; \
 id=1808; \
 revision=1; \
 analyzer(0).name=Squid; \
 analyzer(0).manufacturer=www.squid-cache.org; \
 analyzer(0).class=Proxy; \
 assessment.impact.severity=medium; \
 assessment.impact.type=other; \
 assessment.impact.description=Squid (pid $2) exited; \
 target(0).node.name=$1; \
 target(0).process.name=squid; \
 target(0).process.pid=$2; \
 last
```

here is what it should be:

```
#r11323: Squid Parent: child process 10216 exited due to signal 6
regex=Squid Parent: child process (\d+) exited due to signal (\d); \
 classification.text=Proxy child process stopped; \
 id=1808; \
 revision=2; \
 analyzer(0).name=Squid; \
 analyzer(0).manufacturer=www.squid-cache.org; \
 analyzer(0).class=Proxy; \
 assessment.impact.severity=low; \
 assessment.impact.type=info; \
 assessment.impact.description=A Squid child process (pid $1) exited after reciving a signal $2; \
 target(0).process.name=squid; \
 target(0).process.pid=$1; \
 last
```

History

#1 - 12/15/2006 11:08 AM - Yoann VANDOORSELAERE

- Status changed from New to Assigned

#2 - 12/15/2006 04:18 PM - Yoann VANDOORSELAERE

- Status changed from Assigned to Closed

- Resolution set to fixed

Fixed in r8653. I modified your regexp slightly, corrected the invalid 'info' impact type, kept medium severity (if you have good reason to decrease the severity, then it should be discussed), and don't set the process name statically.

#3 - 04/29/2009 12:27 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude-LML

- Category deleted (4)

- Target version deleted (0.9.8)