Prelude Correlator - Bug #332

Error about missing arguments in prelude-correlator lua ruleset

11/12/2008 03:56 PM -

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.9.0		
Resolution:	fixed		

Description

The warning :

prelude prelude-correlator: ERROR: LUA error on 'business_hour': /etc/prelude-correlator/lua-rules/business-hour.lua:31: set(): require 3 arguments, got
2. (lua.c:148 lua_run)

Looking at other lua ruletset, set() only got 2 arguments ...

History

#1 - 11/20/2008 02:48 PM - Yoann VANDOORSELAERE

Thanks for reporting this issue, could you please let us know the prelude-correlator version being used?

#2 - 11/20/2008 03:04 PM -

prelude correlator 0.9.0-beta3 on RHEL 5.2 with latest libprelude et libpreludedb.

Thks.

#3 - 11/20/2008 03:27 PM - Yoann VANDOORSELAERE

Could you check that the currently installed rule look like the following:

```
function business_hour(INPUT)

local t = INPUT:get("alert.create_time")
local is_succeeded = INPUT:match("alert.assessment.impact.completion", "succeeded")

-- Run this code only on saturday (1) and sunday (6), or from 6:00pm to 9:00am.
if is_succeeded and (t.wday == 1 or t.wday == 6 or t.hour < 9 or t.hour > 18) then
        local ca = IDMEF.new()

        ca:set("alert.source", INPUT:getraw("alert.source"))
        ca:set("alert.target", INPUT:getraw("alert.target"))
        ca:set("alert.classification", INPUT:getraw("alert.classification"))
        ca:set("alert.correlation_alert.alertident(>>).alertident", INPUT:getraw("alert.messageid"))
        ca:set("alert.correlation_alert.alertident(-1).analyzerid", INPUT:getAnalyzerid())
        ca:set("alert.correlation_alert.name", "Critical system activity on day off")
        ca:alert()
end

end
```

#4 - 11/20/2008 05:00 PM -

Hello,

Yes it does.

#5 - 11/21/2008 03:31 PM - Yoann VANDOORSELAERE

I am not able to reproduce the problem here. What LUA version are you using?

#6 - 11/21/2008 07:19 PM -

Hello,

This package http://download.fedora.redhat.com/pub/epel/5/i386/repoview/lua.html on RHEL 5.2.

For the moment, I can't investigate further (correlation is not the priority at the moment) but when i will be working on it full time after posting patches for Fortinet and [[NetScreen]] ruleset for prelule-lml, I will post further information after the debug session.

Thks.

#7 - 02/06/2009 04:59 AM -

I'm seeing the same thing, except I'm running prelude-correlator on Fedora 10, using the Fedora packages.

#8 - 02/06/2009 07:02 AM -

After looking at the source code it seems to me that the problem is actually in IDMEF_getraw. There are circumstances where IDMEF_getraw can return zero values on the stack, thereby causing what looks like:

```
ca:set("alert.source", INPUT:getraw("alert.source"))
```

to execute like it's:

```
ca:set("alert.source")
```

I haven't tested it yet, but changing IDMEF_getraw so that it returns a Lua nil value if idmef_path_get returns zero values should fix things up:

```
diff --git a/plugins/lua/lua-idmef.c b/plugins/lua/lua-idmef.c
index ebde74a..09e82c9 100644
--- a/plugins/lua/lua-idmef.c
+++ b/plugins/lua/lua-idmef.c
@@ -320,8 +320,10 @@ static int IDMEF_getraw(lua_State *lstate)
                return -1;
        }

-       if ( ret == 0 )
-               return 0;
+       if ( ret == 0 ) {
+               lua_pushnil(lstate);
+               return 1;
+       }

        pushIDMEFValue(lstate, value);
        return 1;
```

#9 - 02/06/2009 07:26 AM -

I've added the above patch to my prelude-correlator install and it seems to be working.

#10 - 04/03/2009 10:59 AM - Yoann VANDOORSELAERE

- Status changed from New to Closed

- Resolution set to fixed

Thanks for the patch ! It has been applied in changeset r11109.

#11 - 04/29/2009 12:20 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude Correlator

- Category deleted (11)

- Target version deleted (91)