

Prewikka - Bug #346

Event tab : Prewikka Internal Error

04/07/2009 12:24 PM -

Status:	Resolved	Start date:	
Priority:	Normal	Due date:	
Assignee:	Yoann VANDOORSELAERE	% Done:	100%
Category:		Estimated time:	0.00 hour
Target version:	0.9.15		
Resolution:			

Description

Same defect than [#273](#) under debian Lenny... (no rights to reopen..)

ii	libprelude2	0.9.21.3-2	Hybrid Intrusion Detection System [Base l ibrary]
ii	libpreludedb0	0.9.15.1-3	Hybrid Intrusion Detection System [Base l ibrary]
ii	prelude-correlator	0.9.0~beta3-1	Hybrid Intrusion Detection System [Correl ator]
iU	prelude-lml	0.9.14-2	Hybrid Intrusion Detection System [Log Mo nitoring Lackey]
ii	prelude-manager	0.9.14.2-2	Hybrid Intrusion Detection System [Report Manager]
ii	prewikka	0.9.14-2	Graphical analysis console for the Prelude IDS Framework
ii	python-prelude	0.9.21.3-2	Hybrid Intrusion Detection System [Base l ibrary]
ii	python-preludedb	0.9.15.1-3	Hybrid Intrusion Detection System [Base l ibrary]

Re-Paste the error:

```
Prewikka internal error  
in method 'preludedb_get_alert_idents2', argument 2 of type 'idmef_criteria_t *'
```

Traceback (most recent call last):

```
File "/usr/lib/python2.5/site-packages/prewikka/Core.py", line 333, in process  
    getattr(view_object, view[[handler]]) ()  
File "/usr/lib/python2.5/site-packages/prewikka/views/alertlisting.py", line 1111, in render  
    total = self._setMessages(criteria)  
File "/usr/lib/python2.5/site-packages/prewikka/views/alertlisting.py", line 1067, in _setMessag  
es  
    return self._setAggregatedMessagesNoValues(criteria, ag_s, ag_t, ag_c, ag_a)  
File "/usr/lib/python2.5/site-packages/prewikka/views/alertlisting.py", line 1019, in _setAggreg  
atedMessagesNoValues  
    self._getMissingAggregatedInfos(message, valueshash, parameters, criteria2, aggregated_count)  
File "/usr/lib/python2.5/site-packages/prewikka/views/alertlisting.py", line 885, in _getMissing  
AggregatedInfos  
    message.set_message(self._fetchMessage(ident), ident)  
File "/usr/lib/python2.5/site-packages/prewikka/views/alertlisting.py", line 607, in setMessage  
    self._setMessageAlertIdentInfo(message, message[alertcorrelation_alert], ident)  
File "/usr/lib/python2.5/site-packages/prewikka/views/alertlisting.py", line 545, in _setMessage  
AlertIdentInfo  
    self._fetchInfoFromLinkedMessage(" || ".join(criteria), source, target)  
File "/usr/lib/python2.5/site-packages/prewikka/views/alertlisting.py", line 499, in _fetchInfoF  
romLinkedMessage  
    result = self.env.idmef_db.getAlertIdents(criteria)
```

```
File "/usr/lib/python2.5/site-packages/prewikka/IDMEFDatabase.py", line 402, in getAlertIdsents
    return self._getMessageIdsents(preludedb_get_alert_idsents2, criteria, limit, offset, order_by)
File "/usr/lib/python2.5/site-packages/prewikka/IDMEFDatabase.py", line 388, in _getMessageIdent
s
    result = get_message_idsents(self._db, criteria, limit, offset, order_by)
[[TypeError]]: in method 'preludedb_get_alert_idsents2', argument 2 of type 'idmef_criteria_t *'
```

I get the error when alerting something through a prelude-correlator lua rule. Before that, prewikka is clear.
At first correlation alert, unable to display events (got the error) and if the correlation alert pass the watching period, the display with other events come back...

Related issues:

Duplicated by Prewikka - Bug #273: Error after login into prewikka

Resolved

Associated revisions

Revision 636fd5f8 - 06/10/2009 12:53 PM - Yoann VANDOORSELAERE

Fix IDMEFDatabase exception on empty criteria string.

Providing an empty criteria string as argument to `_getMessageIdsents` used to generate a SWIG pointer mismatch exception. Empty criteria string are now checked for and converted to `None`. This fixes #346.

History

#1 - 04/29/2009 12:21 PM - Yoann VANDOORSELAERE

- Project changed from *PRELUDE SIEM* to *Prewikka*
- Category deleted (5)

#2 - 06/10/2009 12:54 PM - Yoann VANDOORSELAERE

- Status changed from *New* to *Resolved*
- % Done changed from 0 to 100

Applied in changeset [636fd5f854f30a79f9c3989f33e4bf87b7c603ea](#).

#3 - 06/10/2009 12:56 PM - Yoann VANDOORSELAERE

- Assignee set to *Yoann VANDOORSELAERE*
- Target version set to *0.9.15*