LibpreludeDB - Bug #143

prelude-manager overstepping varchar(255) field

04/12/2006 03:51 PM -

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:	worksforme		

Description

Hi,

I have been finding log messages like this since I installed prelude a month ago:

```
prelude-manager: could not insert message into database: Query error: ERROR:  value too long for t
ype character varying(255)
```

I think the manager is trying to insert data that's the wrong size (and perhaps, since postgres is more strict than [[MySQL]], I'm actually getting an error). I can't tell if this is really prelude-manager's fault, but since the manager is the last step before database insertion, I am assuming that it should make sure that the input is formatted correctly.

Here's some information on my setup:

prelude-manager-0.9.1
libpreludedb-0.9.2
libprelude-0.9.3
postgresql-8.1.3
snort-2.4.3
prelude-lml-0.9.1

I have a few snort sensors attached to prelude as well as prelude-lml. I started running prelude-manager with -D 9 to see if I can catch some more info next time this happens, but if anyone here has some ideas please let me know.

History

#1 - 04/17/2006 10:23 AM - Yoann VANDOORSELAERE

- Status changed from New to Assigned

#2 - 04/21/2006 12:42 PM - Yoann VANDOORSELAERE

Could you please edit your manager configuration file, and in the database configuration section, add the following settings:

```
log = /tmp/manager-query.log
```

Then arrange to reproduce the issue, and provide the last SQL query available from the log file before the problem happened.

Thanks,

#3 - 05/31/2006 10:52 PM -

I had the chance to try this again on a new system. here's some information:

This is a sample of the errors from the log file (note how they're not all the same):

May 29 08:00:02 locsrc@globemaster prelude-manager: could not insert message into database: Query error: ERROR: value too long for type character varying(255) .
May 30 08:00:02 locsrc@globemaster prelude-manager: could not insert message into database: Query error: ERROR: value too long for type character varying(255) .
May 31 08:00:02 locsrc@globemaster prelude-manager: could not insert message into database: Query error: ERROR: value too long for type character varying(255) .
May 31 15:10:52 locsrc@globemaster prelude-manager: could not insert message into database: Query error: ERROR: value too long for type character varying(8) .
May 31 15:10:52 locsrc@globemaster prelude-manager: could not insert message into database: Query error: ERROR: value too long for type character varying(8) .
May 31 16:09:25 locsrc@globemaster prelude-manager: could not insert message into database: ERROR: value too long for type character varying(8).
May 31 16:12:38 locsrc@globemaster prelude-manager: could not insert message into database: ERROR: value too long for type character varying(8).
May 31 16:28:47 locsrc@globemaster prelude-manager: could not insert message into database: ERROR: invalid input syntax for type bytea.
May 31 16:28:47 locsrc@globemaster prelude-manager: could not insert message into database: ERROR: invalid input syntax for type bytea.

It's hard to get you good output from manager-query.log since in the 2 or 3 minutes that I ran it, the log file grew to 115MB! Since there were thousands of logs for bytea errors, the following output is likely related to those (sensitive stuff carefully changed to keep character lengths):

0.000s BEGIN
0.000s INSERT INTO Prelude_Alert (messageid) VALUES
0.000s SELECT max(_ident) FROM Prelude_Alert;
0.000s INSERT INTO Prelude_CreateTime (_parent_type, _message_ident, time, gmtoff, usec) VALUES
0.000s INSERT INTO Prelude_DetectTime (_message_ident, time, gmtoff, usec) VALUES
0.000s INSERT INTO Prelude_AnalyzerTime (_parent_type, _message_ident, time, gmtoff, usec) VALUES
0.000s INSERT INTO Prelude_Assessment (_message_ident) VALUES
0.000s INSERT INTO Prelude_Impact (_message_ident, severity, completion, type, description) VALUES
0.000s INSERT INTO Prelude_Analyzer (_parent_type, _message_ident, _index, analyzerid, name, manufacturer, model, version, class, ostype, osversion) VALUES
0.000s INSERT INTO Prelude_Process (_parent_type, _message_ident, _parent0_index, ident, name, pid, path) VALUES
0.000s INSERT INTO Prelude_Analyzer (_parent_type, _message_ident, _index, analyzerid, name, manufacturer, model, version, class, ostype, osversion) VALUES
0.000s INSERT INTO Prelude_Process (_parent_type, _message_ident, _parent0_index, ident, name, pid, path) VALUES
0.000s INSERT INTO Prelude_Analyzer (_parent_type, _message_ident, _index, analyzerid, name, manufacturer, model, version, class, ostype, osversion) VALUES
0.000s INSERT INTO Prelude_Node (_parent_type, _message_ident, _parent0_index, ident, category, location, name) VALUES
0.000s INSERT INTO Prelude_Process (_parent_type, _message_ident, _parent0_index, ident, name, pid, path) VALUES
0.000s INSERT INTO Prelude_Analyzer (_parent_type, _message_ident, _index, analyzerid, name, manufacturer, model, version, class, ostype, osversion) VALUES
0.000s INSERT INTO Prelude_Node (_parent_type, _message_ident, _parent0_index, ident, category, location, name) VALUES
0.000s INSERT INTO Prelude_Process (_parent_type, _message_ident, _parent0_index, ident, name, pid, path) VALUES
0.000s INSERT INTO Prelude_Source (_message_ident, _index, ident, spoofed, interface) VALUES
0.000s INSERT INTO Prelude_User (_parent_type, _message_ident, _parent0_index, ident, category) VALUES
0.000s INSERT INTO Prelude_UserId (_parent_type, _message_ident, _parent0_index, _parent1_index, _parent2_index, _index, ident, type, name, number, tty) VALUES
0.000s INSERT INTO Prelude_UserId (_parent_type, _message_ident, _parent0_index, _parent1_index, _parent2_index, _index, ident, type, name, number, tty) VALUES
0.000s INSERT INTO Prelude_UserId (_parent_type, _message_ident, _parent0_index, _parent1_index, _parent2_index, _index, ident, type, name, number, tty) VALUES
0.000s INSERT INTO Prelude_Source (_message_ident, _index, ident, spoofed, interface) VALUES
0.000s INSERT INTO Prelude_User (_parent_type, _message_ident, _parent0_index, ident, category) VALUES
0.000s INSERT INTO Prelude_UserId (_parent_type, _message_ident, _parent0_index, _parent1_index, _parent2_index, _index, ident, type, name, number, tty) VALUES
0.000s INSERT INTO Prelude_UserId (_parent_type, _message_ident, _parent0_index, _parent1_index, _parent2_index, _index, ident, type, name, number, tty) VALUES
0.000s INSERT INTO Prelude_UserId (_parent_type, _message_ident, _parent0_index, _parent1_index, _parent2_index, _index, ident, type, name, number, tty) VALUES
0.000s INSERT INTO Prelude_Target (_message_ident, _index, ident, decoy, interface) VALUES
0.000s INSERT INTO Prelude_Node (_parent_type, _message_ident, _parent0_index, ident, category, location, name) VALUES
0.000s INSERT INTO Prelude_Process (_parent_type, _message_ident, _parent0_index, ident, name, pid, path) VALUES
0.000s INSERT INTO Prelude_Target (_message_ident, _index, ident, decoy, interface) VALUES
0.000s INSERT INTO Prelude_Node (_parent_type, _message_ident, _parent0_index, ident, category, location, name) VALUES
0.000s INSERT INTO Prelude_Process (_parent_type, _message_ident, _parent0_index, ident, name, pid, path) VALUES
0.000s INSERT INTO Prelude_Classification (_message_ident, ident, text) VALUES
0.000s INSERT INTO Prelude_AdditionalData (_parent_type, _message_ident, _index, type, meaning, data) VALUES
0.000s INSERT INTO Prelude_AdditionalData (_parent_type, _message_ident, _index, type, meaning, data) VALUES Logon Type:3 ')
0.000s ROLLBACK
0.000s BEGIN

0.000s INSERT INTO Prelude_Alert (messageid) VALUES
0.000s SELECT max(_ident) FROM Prelude_Alert;
0.000s INSERT INTO Prelude_CreateTime (_parent_type, _message_ident, time, gmtoff, usec) VALUES
0.000s INSERT INTO Prelude_DetectTime (_message_ident, time, gmtoff, usec) VALUES
0.000s INSERT INTO Prelude_AnalyzerTime (_parent_type, _message_ident, time, gmtoff, usec) VALUES
0.000s INSERT INTO Prelude_Assessment (_message_ident) VALUES
0.000s INSERT INTO Prelude_Impact (_message_ident, severity, completion, type, description) VALUES
0.000s INSERT INTO Prelude_Analyzer (_parent_type, _message_ident, _index, analyzerid, name, manufacturer, model, version, class, ostype, osversion) VALUES
0.000s INSERT INTO Prelude_Process (_parent_type, _message_ident, _parent0_index, ident, name, pid, path) VALUES
0.000s INSERT INTO Prelude_Analyzer (_parent_type, _message_ident, _index, analyzerid, name, manufacturer, model, version, class, ostype, osversion) VALUES
0.000s INSERT INTO Prelude_Process (_parent_type, _message_ident, _parent0_index, ident, name, pid, path) VALUES
0.000s INSERT INTO Prelude_Analyzer (_parent_type, _message_ident, _index, analyzerid, name, manufacturer, model, version, class, ostype, osversion) VALUES
0.000s INSERT INTO Prelude_Node (_parent_type, _message_ident, _parent0_index, ident, category, location, name) VALUES
0.000s INSERT INTO Prelude_Process (_parent_type, _message_ident, _parent0_index, ident, name, pid, path) VALUES
0.000s INSERT INTO Prelude_Analyzer (_parent_type, _message_ident, _index, analyzerid, name, manufacturer, model, version, class, ostype, osversion) VALUES
0.000s INSERT INTO Prelude_Node (_parent_type, _message_ident, _parent0_index, ident, category, location, name) VALUES
0.000s INSERT INTO Prelude_Process (_parent_type, _message_ident, _parent0_index, ident, name, pid, path) VALUES
0.000s INSERT INTO Prelude_Source (_message_ident, _index, ident, spoofed, interface) VALUES
0.000s INSERT INTO Prelude_User (_parent_type, _message_ident, _parent0_index, ident, category) VALUES
0.000s INSERT INTO Prelude_UserId (_parent_type, _message_ident, _parent0_index, _parent1_index, _parent2_index, _index, ident, type, name, number, tty) VALUES
0.000s INSERT INTO Prelude_UserId (_parent_type, _message_ident, _parent0_index, _parent1_index, _parent2_index, _index, ident, type, name, number, tty) VALUES
0.000s INSERT INTO Prelude_UserId (_parent_type, _message_ident, _parent0_index, _parent1_index, _parent2_index, _index, ident, type, name, number, tty) VALUES
0.000s INSERT INTO Prelude_Source (_message_ident, _index, ident, spoofed, interface) VALUES
0.000s INSERT INTO Prelude_User (_parent_type, _message_ident, _parent0_index, ident, category) VALUES
0.000s INSERT INTO Prelude_UserId (_parent_type, _message_ident, _parent0_index, _parent1_index, _parent2_index, _index, ident, type, name, number, tty) VALUES
0.000s INSERT INTO Prelude_UserId (_parent_type, _message_ident, _parent0_index, _parent1_index, _parent2_index, _index, ident, type, name, number, tty) VALUES
0.000s INSERT INTO Prelude_UserId (_parent_type, _message_ident, _parent0_index, _parent1_index, _parent2_index, _index, ident, type, name, number, tty) VALUES
0.000s INSERT INTO Prelude_Target (_message_ident, _index, ident, decoy, interface) VALUES
0.000s INSERT INTO Prelude_Node (_parent_type, _message_ident, _parent0_index, ident, category, location, name) VALUES
0.000s INSERT INTO Prelude_Process (_parent_type, _message_ident, _parent0_index, ident, name, pid, path) VALUES
0.000s INSERT INTO Prelude_Target (_message_ident, _index, ident, decoy, interface) VALUES
0.000s INSERT INTO Prelude_Node (_parent_type, _message_ident, _parent0_index, ident, category, location, name) VALUES
0.000s INSERT INTO Prelude_Process (_parent_type, _message_ident, _parent0_index, ident, name, pid, path) VALUES
0.000s INSERT INTO Prelude_Classification (_message_ident, ident, text) VALUES
0.000s INSERT INTO Prelude_AdditionalData (_parent_type, _message_ident, _index, type, meaning, data) VALUES
0.000s INSERT INTO Prelude_AdditionalData (_parent_type, _message_ident, _index, type, meaning, data) VALUES Logon Type:3 ')
0.000s ROLLBACK

I can't tell what logs are causing these right now... perhaps it was this:

May 31 16:28:42 abcdef/abcdef security[success] 538 DOMAINE\Administrator User Logoff: User Name:Administrator Domain:DOMAINE Logon ID:(0x0,0xFEEF9D) Logon Type:3

Let me know if you need any more info.

#4 - 06/01/2006 01:18 PM - Yoann VANDOORSELAERE

Eric, could you please try the attached patch and report whether it fix your problem ?

#5 - 06/01/2006 04:05 PM -

The patch failed, I forgot to mention that am using the following versions:

libpreludedb: 0.9.5.1
libprelude: 0.9.5
prelude-manager: 0.9.3
prelude-lml: 0.9.2

#6 - 06/01/2006 04:23 PM -

I was able to apply the patch successfully (I was doing it wrong before), and I think it fixes the problems. I ran lml for a few seconds, it captured thousands of alerts, and I didn't see any more bytea/varchar errors in the logs (no more rollbacks in the manager log either).

Thanks!

#7 - 06/01/2006 04:27 PM - Yoann VANDOORSELAERE

- Status changed from Assigned to Closed

- Resolution set to fixed

(In r8224) Always use prelude_escape_binary() when we're inserting additional data. This is
important even in case we're inserting a string, since the database field might be
of a type that require binary kind of escaping. Fix #143.

#8 - 06/01/2006 04:29 PM - Yoann VANDOORSELAERE

By the way, the comments doesn't fit the summary of this bug.
You were originally reporting the following error:

```
prelude-manager: could not insert message into database: Query error: ERROR:  value too long for type characte
r varying(255)
```

Are you able to reproduce this ?

#9 - 06/01/2006 05:19 PM -

I have been looking through the alerts from lml in prewikka, and I noticed that in sections like Additional Data, stuff looks like this:

Log received from /var/log/abc.snare\000
Original Log Jun 1 09:15:46 abc/abc security[success] 680 NT AUTHORITY\\SYSTEM Account Used for Logon by:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Account Name: abcdefg Workstation: AB-CD \000

Are the trailing \000's a result of this patch?

#10 - 06/01/2006 05:24 PM - Yoann VANDOORSELAERE

Yes, this is fixed in r8225

#11 - 06/12/2006 04:52 PM -

- Status changed from Closed to Feedback

- Resolution deleted (fixed)

I just got more messages like this in my logs using the most recent versions:

Jun 12 10:54:55 globemaster prelude-manager: could not insert message into database: ERROR: value too long for type character varying(255).

Will try to hunt down the source...

#12 - 06/12/2006 04:54 PM - Yoann VANDOORSELAERE

Please watch at the SQL query log and report the statement preceding the ROLLBACK.
Regards,

#13 - 05/02/2007 02:48 PM - Yoann VANDOORSELAERE

- Status changed from Feedback to Closed

- Resolution set to worksforme

Closing this issue due to lack of feedback. Please re-open if appropriate.

#14 - 04/29/2009 12:23 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to LibpreludeDB

- Category deleted (2)

- Target version deleted (0.9.8)

Files

preludedb-data.diff	1.52 KB	06/01/2006	Yoann VANDOORSELAERE