Suricata - Bug #1670

Modbus compiler warnings on Fedora 23

01/16/2016 11:23 AM - Peter Manev

Status: Closed
Priority: Normal
Assignee: David DIALLO
Category:
Target version: 3.0.1RC1
Affected Versions:
Effort:

Description
When compiling 3.0RC3 from source on Fedora 23 -

```
[root@localhost suricata-3.0RC3]# uname -a
Linux localhost.localdomain 4.2.7-300.fc23.x86_64 #1 SMP Wed Dec 9 22:28:30 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
```

the following warnings are present about modbus:

```
CC        app-layer-modbus.o
app-layer-modbus.c: In function 'ModbusParseWriteRequest':
app-layer-modbus.c:736:31: warning: 'byte' may be used uninitialized in this function [-Wmaybe-uninitialized]
  tx->data[i] = (uint16_t) byte;
^
app-layer-modbus.c: In function 'ModbusParseResponse':
app-layer-modbus.c:614:24: warning: 'count' may be used uninitialized in this function [-Wmaybe-uninitialized]
  (count != (2 * (tx->read.quantity))))
  ^
app-layer-modbus.c:599:13: note: 'count' was declared here
  uint8_t count;
  ^
app-layer-modbus.c:1164:24: warning: 'mei' may be used uninitialized in this function [-Wmaybe-uninitialized]
  if (mei != tx->mei)
  ^
app-layer-modbus.c:1121:49: note: 'mei' was declared here
  uint8_t count, error = FALSE, function, mei;
  ^
app-layer-modbus.c:1156:21: warning: 'count' may be used uninitialized in this function [-Wmaybe-uninitialized]
  ModbusCheckHeaderLength(modbus, tx->length, 2 + count);
  ^
app-layer-modbus.c:1121:17: note: 'count' was declared here
  uint8_t count, error = FALSE, function, mei;
  ^
app-layer-modbus.c:499:5: warning: 'exception' may be used uninitialized in this function [-Wmaybe-uninitialized]
  switch (exception) {
  ^
app-layer-modbus.c:493:13: note: 'exception' was declared here
  uint8_t exception;
  ^
app-layer-modbus.c:1138:13: warning: 'function' may be used uninitialized in this function [-Wmaybe-uninitialized]
  switch(function) {
  ^
app-layer-modbus.c:1121:39: note: 'function' was declared here
  uint8_t count, error = FALSE, function, mei;
```
app-layer-modbus.c: In function 'ModbusParseRequest':
app-layer-modbus.c:1040:13: warning: 'count' may be used uninitialized in this function [-Wmaybe-uninitialized]
    ModbusCheckHeaderLength(modbus, tx->length, 2 + count);
^  
app-layer-modbus.c:964:17: note: 'count' was declared here
    uint8_t count;
^  

History
#1 - 01/17/2016 06:27 AM - Victor Julien
- Tracker changed from Optimization to Bug
- Status changed from Feedback to Assigned
- Assignee changed from Jason Ish to David DIALLO
- Target version set to 70

David, can you have a look at this?

#2 - 01/17/2016 06:28 AM - Victor Julien
- Description updated

Cleaned up description.

#3 - 01/17/2016 06:29 AM - Victor Julien
- Subject changed from Modbus warnings - when compiling on Fedora 23 to Modbus compiler warnings on Fedora 23

#4 - 02/25/2016 03:09 AM - David DIALLO
All Modbus warnings generated when compiling 3.0RC3 from source on Fedora 23 are not releavants.

In fact, all variables are initialized thanks to ModbusExtractUint8 or ModbusExtractUint16 function that extracts 8bits or 16bits data from pointer the received input data. In case of extracting error (because of length), ModbusExtractUint8 or ModbusExtractUint16 returns an error that is managed by the caller function.

In any case, all variables can be initialized to zero when they are declared. It does not change anything functionally but it will remove Modbus warnings.

#5 - 02/25/2016 04:07 AM - David DIALLO
- Due date set to 02/25/2016
- Status changed from Assigned to Resolved
- % Done changed from 0 to 100

#6 - 02/26/2016 09:26 AM - Victor Julien
- Status changed from Resolved to Closed
- Target version changed from 70 to 3.0.1RC1

https://github.com/inliniac/suricata/commit/3a3cc43f6a81eba3175d35b1843c57896f591238