Suricata - Bug #600

literal \t (x09) in mod_log_config

10/11/2012 02:59 PM - Erik C

Status: Closed
Priority: Normal
Assignee: Ignacio Sanchez
Category:
Target version:
Affected Versions:
Effort:
Difficulty:
Label:

Description
When reporting data out via mod_log_config for http.log, I have discovered that \t is reported as \x09. Per apache.org....
---
For security reasons, starting with version 2.0.46, non-printable and other special characters in %r, %i and %o are escaped using \xhh sequences, where hh stands for the hexadecimal representation of the raw byte.... Exceptions from this rule are....all whitespace characters, which are written in their C-style notation ('\n', '\t', etc).
---
Why are my customformat strings producing x09 in Suricata, when according to mod_log_config (which suri points you to) indicates that these should be printed as is, and not hex?

Thanks!
Erik

Related issues:
Related to Feature #602: availability for http.log output - identical to apac... Closed 10/29/2012

History
#1 - 10/12/2012 02:46 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Ignacio Sanchez

#2 - 10/12/2012 03:36 AM - Ignacio Sanchez
The special characters are escaped by the libhtp library. I understand that Apache mod_log_config behaves slightly different, but suricata customhttplog was never meant (at least not for now) to replicate exactly mod_log_config behavior.

It is merely "inspired" by its syntax. In fact, there are some/many features such as %C not yet implemented (working on it...).

The wiki page is perhaps a little bit misleading in this regard (https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Custom_http_logging). I will change it to include a more detailed explanation.

The Feature #530 describes better the capabilities of customhttplog and its relation with mod_log_config. (https://redmine.openinfosecfoundation.org/issues/530#change-2101)

#3 - 10/12/2012 03:49 AM - Peter Manev
Thank you Ignacio.
I also noticed actually - that when using custom (Apache style) http.log - the resulting log could not exactly be parsed as a lot of apache log parsers would normally do for apache itself - is it supposed work that way? Just wondering.

#4 - 10/12/2012 04:18 AM - Ignacio Sanchez
As I said I never meant at this point to allow the production of an output identical to the one of mod_log_config...

Could you try identify what is the difference in the outputs, which causes the problem (perhaps it is the /t /n)? We can add them as feature requests, and look into them for the next enhancement. I am currently preparing one to add support for the extraction of individual cookie values, and maximum length for the extracted fields. I could add some of these missing features there as well.

#5 - 10/12/2012 10:28 AM - Victor Julien
Ignacio Sanchez wrote:

The special characters are escaped by the libhtp library.

They are actually escaped in Suricata itself. Check util-buffer.[ch].

#6 - 10/13/2012 01:23 PM - Erik C
I looked at util-buffer.h and saw the following, which mimics roughly the same behavior of mod_log_config, but not quite:

(from util-buffer.h)
----
Printable characters are written in the printable format and the non-printable chars are written in hex codes using the \XX format.
----

If we could just get \t to print as whitespace and not as a hex code, that would make our lives immesurably wonderful. Thanks for the assist in this! We are looking to move to Suri possibly, and getting this would be the final piece to the puzzle!

#7 - 10/13/2012 03:52 PM - Ignacio Sanchez
I have updated the custom http logging wiki page.

https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Custom_http_logging

Please let me know if you find any errors in the documentation, or if you find the logging behaves in a different way.

#8 - 10/15/2012 03:00 AM - Victor Julien
I think we can easily add another print function to create the format of mod_log_config. Ignacio, are you interested in implementing that?

#9 - 10/16/2012 12:56 PM - Ignacio Sanchez
I think we can easily add another print function to create the format of mod_log_config. Ignacio, are you interested in implementing that?

Yes, ok. The feature request is #602

#10 - 10/26/2013 10:23 AM - Victor Julien
- Target version set to TBD

#11 - 12/22/2015 04:14 PM - Andreas Herz
- Status changed from Assigned to Closed

fixed by #602

#12 - 10/19/2017 12:57 AM - Victor Julien
- Target version deleted (TBD)