Suricata - Bug #903
libhtp valgrind warning
07/25/2013 02:18 AM - Victor Julien

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category: 
Target version: 2.0beta2
Affected Versions:
Difficulty:
Effort:
Label:

Description

==11894== Thread 8:
==11894== Conditional jump or move depends on uninitialised value(s)
==11894==    at 0x60B7B8A0: htp_tx_urldecode_uri_inplace (htp_util.c:1427)
==11894==    by 0x60B7E97: htp_normalize_parsed_uri (htp_util.c:1690)
==11894==    by 0x60B4C5C: htp_tx_state_request_line (htp_transaction.c:937)
==11894==    by 0x60B0D36: htp_connp_REQ_LINE (htp_request.c:706)
==11894==    by 0x60B0E78: htp_connp_req_data (htp_request.c:851)
==11894==    by 0x456968: HTPHandleRequestData (app-layer-htp.c:642)
==11894==    by 0x47F111: AppLayerDoParse (app-layer-parser.c:894)
==11894==    by 0x48061E: AppLayerParse (app-layer-parser.c:1100)
==11894==    by 0x41CFF8: AppLayerHandleTCPData (app-layer.c:161)
==11894==    by 0x8A9499: StreamTcpReassembleAppLayer (stream-tcp-reassemble.c:2933)
==11894==    by 0x8A8CE3: StreamTcpReassembleHandleSegmentUpdateACK (stream-tcp-reassemble.c:3295)
==11894==    by 0x8A8C532: StreamTcpReassembleHandleSegment (stream-tcp-reassemble.c:3369)
==11894==
==11894== Conditional jump or move depends on uninitialised value(s)
==11894==    at 0x60B7BB3: htp_tx_urldecode_uri_inplace (htp_util.c:1431)
==11894==    by 0x60B7E97: htp_normalize_parsed_uri (htp_util.c:1690)
==11894==    by 0x60B4C5C: htp_tx_state_request_line (htp_transaction.c:937)
==11894==    by 0x60B0D36: htp_connp_REQ_LINE (htp_request.c:706)
==11894==    by 0x60B0E78: htp_connp_req_data (htp_request.c:851)
==11894==    by 0x456968: HTPHandleRequestData (app-layer-htp.c:642)
==11894==    by 0x47F111: AppLayerDoParse (app-layer-parser.c:894)
==11894==    by 0x48061E: AppLayerParse (app-layer-parser.c:1100)
==11894==    by 0x41CFF8: AppLayerHandleTCPData (app-layer.c:161)
==11894==    by 0x8A9499: StreamTcpReassembleAppLayer (stream-tcp-reassemble.c:2933)
==11894==    by 0x8A8CE3: StreamTcpReassembleHandleSegmentUpdateACK (stream-tcp-reassemble.c:3295)
==11894==    by 0x8A8C532: StreamTcpReassembleHandleSegment (stream-tcp-reassemble.c:3369)
==11894==
==11894== Conditional jump or move depends on uninitialised value(s)
==11894==    at 0x60B7BC6: htp_tx_urldecode_uri_inplace (htp_util.c:1435)
==11894==    by 0x60B7E97: htp_normalize_parsed_uri (htp_util.c:1690)
==11894==    by 0x60B4C5C: htp_tx_state_request_line (htp_transaction.c:937)
==11894==    by 0x60B0D36: htp_connp_REQ_LINE (htp_request.c:706)
==11894==    by 0x60B0E78: htp_connp_req_data (htp_request.c:851)
==11894==    by 0x456968: HTPHandleRequestData (app-layer-htp.c:642)
==11894==    by 0x47F111: AppLayerDoParse (app-layer-parser.c:894)
==11894==    by 0x48061E: AppLayerParse (app-layer-parser.c:1100)
==11894==    by 0x41CFF8: AppLayerHandleTCPData (app-layer.c:161)
==11894==    by 0x8A9499: StreamTcpReassembleAppLayer (stream-tcp-reassemble.c:2933)
==11894==    by 0x8A8CE3: StreamTcpReassembleHandleSegmentUpdateACK (stream-tcp-reassemble.c:3295)
==11894==    by 0x8A8C532: StreamTcpReassembleHandleSegment (stream-tcp-reassemble.c:3369)
==11894==
==11894== Conditional jump or move depends on uninitialised value(s)
==11894==    at 0x60B7BC6: htp_tx_urldecode_uri_inplace (htp_util.c:1435)
==11894==    by 0x60B7E97: htp_normalize_parsed_uri (htp_util.c:1690)
==11894==    by 0x60B4C5C: htp_tx_state_request_line (htp_transaction.c:937)
==11894==    by 0x60B0D36: htp_connp_REQ_LINE (htp_request.c:706)
==11894==    by 0x60B0E78: htp_connp_req_data (htp_request.c:851)
==11894==    by 0x456968: HTPHandleRequestData (app-layer-htp.c:642)
==11894==    by 0x47F111: AppLayerDoParse (app-layer-parser.c:894)
==11894==    by 0x48061E: AppLayerParse (app-layer-parser.c:1100)
==11894==    by 0x41CFF8: AppLayerHandleTCPData (app-layer.c:161)
==11894==    by 0x8A9499: StreamTcpReassembleAppLayer (stream-tcp-reassemble.c:2933)
==11894==    by 0x8A8CE3: StreamTcpReassembleHandleSegmentUpdateACK (stream-tcp-reassemble.c:3295)
==11894==    by 0x8A8C532: StreamTcpReassembleHandleSegment (stream-tcp-reassemble.c:3369)
==11894==

This is from running Suri through valgrind on a very large pcap overnight, so extracting the flow is impossible.

History

#1 - 07/25/2013 03:46 AM - Victor Julien

06/13/2020
Trying to isolate the flow(s) using [https://github.com/inliniac/suricata/pull/463](https://github.com/inliniac/suricata/pull/463)

#2 - 07/25/2013 09:28 AM - Ivan Ristic
- Status changed from Assigned to Resolved

This was fixed a couple of days ago, in LibHTP v.0.5.6:
[https://github.com/ironbee/libhtp/commit/2d2105a7225b268f56c46bf41945c32305c21177](https://github.com/ironbee/libhtp/commit/2d2105a7225b268f56c46bf41945c32305c21177)

#3 - 08/29/2013 10:54 PM - Anoop Saldanha
- Status changed from Resolved to Closed
- Assignee changed from Anoop Saldanha to Victor Julien