Problem happens if the split happens in the middle of a record size
Another problems happens if the buffer size is less than 4

Problem found while running suricata-verify tests against Suricata compiled with this patch

diff --git a/src/app-layer.c b/src/app-layer.c
index b614f2712..0149d6b4f 100644
--- a/src/app-layer.c
+++ b/src/app-layer.c
@@ -658,8 +658,15 @@ int AppLayerHandleTCPData(ThreadVars *tv, TcpReassemblyThreadCtx *ra_ctx,
             r = AppLayerParserParse(tv, app_tctx->alp_tctx, f, f->alproto,
             flags, data+i, 1);
         }
+-#ifdef LOLSPLIT
+-    for (size_t i = 0; i < data_len; i++) {
+-        r = AppLayerParserParse(tv, app_tctx->alp_tctx, f, f->alproto, flags, data+i, 1);
+-    }
+#else
+    r = AppLayerParserParse(tv, app_tctx->alp_tctx, f, f->alproto, flags, data, data_len);
+#endif
+
+PACKET_PROFILING_APP_END(app_tctx, f->alproto);

Related issues:
Copied from Bug #3525: Kerberos vulnerable to TCP splitting evasion  Closed
Copied to Bug #3527: 4.1.x Kerberos vulnerable to TCP splitting evasion  Closed

History
#1 - 03/12/2020 12:50 PM - Philippe Antoine
  - Copied from Bug #3525: Kerberos vulnerable to TCP splitting evasion added

#2 - 03/12/2020 12:50 PM - Philippe Antoine
  - Copied to Bug #3527: 4.1.x Kerberos vulnerable to TCP splitting evasion added

#3 - 04/15/2020 05:45 PM - Jeff Lucovsky
  - Status changed from New to Assigned
  - Assignee set to Jeff Lucovsky

#4 - 04/16/2020 05:18 PM - Jeff Lucovsky
  - Status changed from Assigned to In Review

https://github.com/OISF/suricata/pull/4829
- Status changed from In Review to Closed