Suricata - Bug #3615
Protocol detection evasion by packet splitting
04/06/2020 03:19 PM - Philippe Antoine

Status: Closed
Priority: Normal
Assignee: Philippe Antoine
Category: Target version: 6.0.0beta1
Affected Versions: 5.0.2
Effort:

Description
Found by oss-fuzz

Output of fuzz target gives:
Assertion failure: With input length 24, found enip instead of dns
on attached input

Related issues:
Copied to Bug #3671: Protocol detection evasion by packet splitting
Closed
Copied to Bug #3674: Protocol detection evasion by packet splitting
Closed
Copied to Bug #3689: Protocol detection evasion by packet splitting on enip/nfs
Closed

History
#1 - 04/06/2020 03:20 PM - Philippe Antoine
Patch could be to improve the ENIP probing parser

```
diff --git a/src/app-layer-enip.c b/src/app-layer-enip.c
index 282294536..b9e3b32db 100644
--- a/src/app-layer-enip.c
+++ b/src/app-layer-enip.c
@@ -393,8 +393,24 @@
 static uint16_t ENIPProbingParser(Flow *f, uint8_t direction,
     SCLogDebug("length too small to be a ENIP header");
     return ALPROTO_UNKNOWN;

-    return ALPROTO_ENIP;
+    uint16_t cmd;
+    ByteExtractUint16(&cmd, BYTE_LITTLE_ENDIAN, sizeof(uint16_t),
+        (const uint8_t *) (input));
+    switch(cmd) {
+        //fallthrough
+        case NOP:
+            return ALPROTO_ENIP;
+        case LIST_SERVICES:
+            return ALPROTO_ENIP;
+        case LIST_IDENTITY:
+            return ALPROTO_ENIP;
+        case LIST_INTERFACES:
+            return ALPROTO_ENIP;
+        case REGISTER_SESSION:
+            return ALPROTO_ENIP;
+        case UNREGISTER_SESSION:
+            return ALPROTO_ENIP;
+        case SEND_BR_DATA:
+            return ALPROTO_ENIP;
+        case SEND_Unit_DATA:
+            return ALPROTO_ENIP;
+        case INDICATE_STATUS:
+            return ALPROTO_ENIP;
+        case CANCEL:
+            return ALPROTO_ENIP;
+    }
+    return ALPROTO_FAILED;
+
/**
```

#2 - 04/06/2020 04:03 PM - Victor Julien
-Affected Versions 5.0.2 added

05/30/2021 1/2
- Affected Versions deleted (5.0.3)

#3 - 04/10/2020 03:10 PM - Victor Julien
- Status changed from New to In Review
- Assignee set to Philippe Antoine

#4 - 04/15/2020 08:02 AM - Philippe Antoine
- Target version changed from 6.0.0beta1 to 5.0.3

https://gitlab.oisf.net/dev/suricata/-/merge_requests/27

#5 - 04/15/2020 08:02 AM - Philippe Antoine
- Label Needs backport to 4.1 added

#6 - 04/24/2020 11:40 AM - Jeff Lucovsky
- Copied to Bug #3671: Protocol detection evasion by packet splitting added

#7 - 04/24/2020 12:05 PM - Victor Julien
- Target version changed from 5.0.3 to 6.0.0beta1

#8 - 04/24/2020 12:05 PM - Victor Julien
- Copied to Bug #3674: Protocol detection evasion by packet splitting added

#9 - 05/01/2020 09:25 AM - Philippe Antoine
- Status changed from In Review to Closed

https://gitlab.oisf.net/dev/suricata/-/merge_requests/34

https://github.com/OISF/suricata/commit/a15e503b7d30c657d402a12795212d59c8490760

#10 - 05/01/2020 10:53 AM - Victor Julien
- Label deleted (Needs backport to 4.1)

#11 - 05/02/2020 06:20 PM - Philippe Antoine
- Copied to Bug #3689: Protocol detection evasion by packet splitting on enip/nfs added

#12 - 03/15/2021 12:11 PM - Jeff Lucovsky
- Private changed from Yes to No

Files

clusterfuzz-testcase-minimized-fuzz_applayerprotodetectgetproto-5121705677946880.fuzz
34 Bytes
04/06/2020
Philippe Antoine