Suricata - Feature #2860

Suricata doesn't detect part of IKEv2 traffic

03/04/2019 10:30 AM - Michal Vymazal

| Status:     | Assigned          |
| Priority:   | Normal            |
| Assignee:   | Pierre Chifflier  |
| Category:   |                   |
| Target version: | TBD            |
| Effort:     |                   |
| Difficulty: |                   |

**Description**

Suricata doesn't detect part of IKEv2 traffic.

Some devices (Mikrotik for example) allows to start IKEv2 traffic on port 4500 (not affected by NAT Traversal enabled). In the case of UDP 4500 for IKEv2 selected, this IKEv2 traffic is not detected by Suricata. The traffic is detected as normal UDP traffic, but not recognized as IKEv2.

**Mikrotik RB951G-2HNd (mipsbe), RouterOS 6.44**

```bash
# suricata --build-info
This is Suricata version 4.1.0-dev (rev 8709a20d)
Features: NFQ PCAP_SET_BUFF AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1 HAVE_HTP_URI_NORMALIZE E_HOOK PCRE_JIT HAVE_NSS HAVE_LUA HAVE_LUAJIT HAVE_LIBJANSSON TLS MAGIC RUST
SIMD support: none
Atomic intrinsics: 1 2 4 8 byte(s)
64-bits, Little-endian architecture
GCC version 6.3.0 20170516, C version 199901
compiled with _FORTIFY_SOURCE=2
L1 cache line size (CLS)=64
thread local storage method: __thread
compiled with LibHTP v0.5.28, linked against LibHTP v0.5.28
```

**Suricata Configuration:**

- **AF_PACKET support:** yes
- **eBPF support:** no
- **XDP support:** no
- **PF_RING support:** no
- **NFQueue support:** yes
- **NFLOG support:** no
- **IPFW support:** no
- **Netmap support:** no
- **DAG enabled:** no
- **Napatech enabled:** no
- **WinDivert enabled:** no
- **Unix socket enabled:** yes
- **Detection enabled:** yes

- **Libmagic support:** yes
- **libnss support:** yes
- **libnsspr support:** yes
- **libjansson support:** yes
- **liblzma support:** yes
- **hiredis support:** yes
- **hiredis async with libevent:** no
- **Frelude support:** no
- **PCRE jit:** yes
- **LUA support:** yes, through luajit
- **libluajit:** yes
<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>libgeoip</td>
<td>yes</td>
</tr>
<tr>
<td>Non-bundled http</td>
<td>yes</td>
</tr>
<tr>
<td>Old barnyard2 support</td>
<td>no</td>
</tr>
<tr>
<td>Hyperscan support</td>
<td>yes</td>
</tr>
<tr>
<td>Libnet support</td>
<td>yes</td>
</tr>
<tr>
<td>liblz4 support</td>
<td>yes</td>
</tr>
<tr>
<td>Rust support</td>
<td>yes (default)</td>
</tr>
<tr>
<td>Rust strict mode</td>
<td>no</td>
</tr>
<tr>
<td>Rust debug mode</td>
<td>no</td>
</tr>
<tr>
<td>Rust compiler</td>
<td>rustc 1.30.0 (da5f414c2 2018-10-24)</td>
</tr>
<tr>
<td>Rust cargo</td>
<td>cargo 1.30.0 (36d96825d 2018-10-24)</td>
</tr>
<tr>
<td>Install suricatasc</td>
<td>yes</td>
</tr>
<tr>
<td>Install suricata-update</td>
<td>no</td>
</tr>
<tr>
<td>Profiling enabled</td>
<td>no</td>
</tr>
<tr>
<td>Profiling locks enabled</td>
<td>no</td>
</tr>
</tbody>
</table>

**Development settings:**
- Coccinelle / spatch: no
- Unit tests enabled: no
- Debug output enabled: no
- Debug validation enabled: no

**Generic build parameters:**
- Installation prefix: /usr
- Configuration directory: /etc/suricata/
- Log directory: /var/log/suricata/

```
--prefix /usr
--sysconfdir /etc
--localstatedir /var
--datarootdir /usr/share
```

**Host:** x86_64-pc-linux-gnu

**Compiler:** gcc (exec name) / gcc (real)

**History**

**#1 - 03/04/2019 10:32 AM - Victor Julien**
- Description updated

Can you share a pcap of this traffic to reproduce?

**#2 - 03/04/2019 11:08 AM - Michal Vymazal**
- File IKEv2-UDP-4500-IKE_SA_INIT-2.pcap added

Here is the pcap file with IKEv2 traffic on UDP 4500.

This traffic is not detected by the IKEv2 dashboard and also not detected with this rule:

```
alert ikev2 any any -> any any (msg:"IKEv2 IKE_SA_INIT Responder 21 20 22 20";content:"[21 20 22 20]"); classtype:protocol-command-decode;
sid:500072; rev:1;metadata:created_at 2019_02_11, updated_at 2019_02_11;)
alert ikev2 any any -> any any (msg:"IKEv2 IKE_SA_INIT Initiator 28 20 22 08 Next Payload: Nonce";content:"[28 20 22 08]"); classtype:protocol-command-decode; sid:500073; rev:1;metadata:created_at 2019_02_11, updated_at 2019_02_11;)
```

---

09/08/2020
When I turn the IKEv2 traffic back to the UDP 500 port, the IKEv2 traffic will be detected with IKEv2 dashboard and also will be detected with this two suricata rules.

#3 - 03/04/2019 01:55 PM - Victor Julien
- Assignee set to Pierre Chifflier

Hi Pierre, could you check this out?

#4 - 03/06/2019 06:14 PM - Victor Julien
- Tracker changed from Bug to Feature
- Status changed from New to Assigned
- Target version set to 5.0beta1

#5 - 04/25/2019 11:11 AM - Victor Julien
- Target version changed from 5.0beta1 to TBD

Files
IKEv2-UDP-4500-IKE_SA_INIT-2.pcap 1.87 KB 03/04/2019 Michal Vymazal