Suricata - Bug #3324
TCP evasion technique by overlapping a TCP segment with a fake packet
11/06/2019 10:12 PM - Nicolas Adba

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>High</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Victor Julien</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>5.0.1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td>5.0.0</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description
It's possible to bypass/evade any tcp based signature by overlapping a TCP segment with a fake FIN packet.

The fake FIN packet is injected just before the PUSH ACK packet we want to bypass. The PUSH ACK packet (containing the data) will be ignored by suricata because it overlaps the FIN packet (the sequence and ack number are identical in the two packets). The client will ignore the fake FIN packet because the ACK flag is not set.
Both linux and windows client are ignoring the injected packet.

Client  -----------  Legit TCP handshake  -----------  Evil Server
Client  <-  [FIN]  [Seq=80 Ack=100] XXXXXXX  <-  Evil Server  # injected packet with fake data (ignored by the client)
Client  <-  [PUSH, ACK] [Seq=80 Ack=100] MALWARE  <-  Evil Server  # Legit data (ignored by suricata)

This evasion technique is referenced as CVE-2019-18792.

You can find attached :
- test.rule : A tcp rule that detects the string THIS_IS_A_TEST
- without_evasion.pcap : A web server which sends the string THIS_IS_A_TEST to a client without any evasion technique
- with_evasion_windows.pcap : A web server which sends the string THIS_IS_A_TEST to a windows 10 client with this evasion technique
- with_evasion_linux.pcap : A web server which sends the string THIS_IS_A_TEST to a linux client (tested with kernel 5.2.0) with this evasion technique

Related issues:
Copied to Bug #3394: TCP evasion technique by overlapping a TCP segment with a fake packet (4.1.x) added

History

#1 - 11/07/2019 10:03 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to Soon

#2 - 11/08/2019 09:18 AM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Victor Julien

#3 - 11/21/2019 04:28 PM - Victor Julien
- Target version changed from Soon to 5.0.1

#4 - 11/23/2019 09:35 AM - Victor Julien
- Priority changed from Normal to High
- Label Needs backport added

#5 - 12/10/2019 04:20 PM - Victor Julien
- Copied to Bug #3394: TCP evasion technique by overlapping a TCP segment with a fake packet (4.1.x) added

06/13/2020
- Status changed from Assigned to Closed
- Private changed from Yes to No
- Label deleted (Needs backport)

[GitHub Commit Link](https://github.com/OISF/suricata/commit/fa692df37a796c3330c81988d15ef1a219af006)

<table>
<thead>
<tr>
<th>Files</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>without_evasion.pcap</td>
<td>1.01 KB</td>
<td>11/06/2019</td>
<td>Nicolas Adba</td>
</tr>
<tr>
<td>with_evasion_linux.pcap</td>
<td>1.16 KB</td>
<td>11/06/2019</td>
<td>Nicolas Adba</td>
</tr>
<tr>
<td>with_evasion_windows.pcap</td>
<td>1.13 KB</td>
<td>11/06/2019</td>
<td>Nicolas Adba</td>
</tr>
<tr>
<td>test.rule</td>
<td>147 Bytes</td>
<td>11/06/2019</td>
<td>Nicolas Adba</td>
</tr>
</tbody>
</table>