Suricata - Bug #3328

bad ip option evasion

11/07/2019 08:25 PM - Nicolas Adba

Status: Closed
Priority: Normal
Assignee: Jason Ish
Category:
Target version: 5.0.1
Affected Versions: 5.0.0

Description
Suricata is vulnerable to bad ip option evasions. Here are the pcaps of issue number 3286 with a bad ipv4 option.

I don't think it's exploitable in the wild because routers should drop the injected packets (I didn't test it thought).

Related issues:
Copied to Bug #3414: bad ip option evasion (4.1.x) Closed

History
#1 - 11/07/2019 10:04 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to Soon

#2 - 11/14/2019 04:03 PM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Jason Ish
- Target version changed from Soon to 5.0.1

#3 - 11/23/2019 09:34 AM - Victor Julien
- Priority changed from Normal to High
- Label Needs backport added

#4 - 12/13/2019 03:40 PM - Victor Julien
- Status changed from Assigned to Closed
- Priority changed from High to Normal
- Private changed from Yes to No
- Label deleted (Needs backport)

https://github.com/OISF/suricata/commit/df8db1ddb0736300bad4a7fee811d333ab77cb54
https://github.com/OISF/suricata/commit/8609939e60cdd52dc1745e2eeb5dc3db275ac13

#5 - 12/13/2019 03:43 PM - Victor Julien
- Copied to Bug #3414: bad ip option evasion (4.1.x) added

Files

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>with_evasion_windows.pcap</td>
<td>1.26 KB</td>
<td>11/07/2019</td>
<td>Nicolas Adba</td>
</tr>
<tr>
<td>with_evasion_linux.pcap</td>
<td>1.43 KB</td>
<td>11/07/2019</td>
<td>Nicolas Adba</td>
</tr>
<tr>
<td>without_evasion.pcap</td>
<td>1.01 KB</td>
<td>11/07/2019</td>
<td>Nicolas Adba</td>
</tr>
<tr>
<td>test.rule</td>
<td>147 Bytes</td>
<td>11/07/2019</td>
<td>Nicolas Adba</td>
</tr>
</tbody>
</table>