Suricata - Bug #3286

TCP evasion technique by faking a closed TCP session

10/29/2019 07:50 PM - Nicolas Adba

Status:	Closed		
Priority:	Normal		
Assignee:	Victor Julien		
Category:			
Target version:	5.0.1		
Affected Versions:	5.0.0	**Difficulty:**	
Effort:		**Label:**	

Description

It is possible to bypass/evade any tcp based signature by faking a closed TCP session using an evil server.
After the TCP SYN packet, it's possible to inject a RST ACK and a FIN ACK packet with an old TCP Timestamp option.
The client will ignore the RST ACK and the FIN ACK packets because of the old TCP Timestamp option.
Both linux and windows client are ignoring the injected packets.

```
Client    ->  [SYN] [Seq=0 Ack=0]                                    ->  Evil Server     # Legit
TCP handshake
Client    <-  [RST, ACK] [Seq=0 Ack=1] [old TCP Timestamp option]    <-  Evil Server     # Inject
ed packet
Client    <-  [FIN, ACK] [Seq=0 Ack=1] [old TCP Timestamp option]    <-  Evil Server     # Inject
ed packet
Client    <-  [SYN, ACK] [Seq=0 Ack=1]                               <-  Evil Server     # Legit
TCP handshake
Client    <-  [ACK] [Seq=1 Ack=1]                                    <-  Evil Server     # Legit
TCP handshake
Client    ===============  Data evasion        =================          Evil Server
```

This evasion technique is referenced as CVE-2019-18625.

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 (kernel 5.2.0) with this evasion technique

Related issues:

Copied to Bug #3395: TCP evasion technique by faking a closed TCP session (4....	**Closed**

History

#1 - 11/01/2019 08:23 AM - Victor Julien

- Private changed from No to Yes

#2 - 11/01/2019 08:24 AM - Victor Julien

- Description updated

- Status changed from New to Assigned

- Assignee set to Victor Julien

- Target version set to 5.0.1

- Label Needs backport added

#3 - 11/23/2019 09:35 AM - Victor Julien

- Priority changed from Normal to High

#4 - 12/10/2019 04:20 PM - Victor Julien

- Copied to Bug #3395: TCP evasion technique by faking a closed TCP session (4.1.x) added

#5 - 12/13/2019 03:39 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/9f0294fadca3dcc18c919424242a41e01f3e8318

Files

test.rule	147 Bytes	10/29/2019	Nicolas Adba
with_evasion_windows.pcap	1.12 KB	10/29/2019	Nicolas Adba
with_evasion_linux.pcap	1.24 KB	10/29/2019	Nicolas Adba
without_evasion.pcap	1.01 KB	10/29/2019	Nicolas Adba