Suricata - Support #3197

suricata dropping traffic on alert

09/27/2019 02:25 AM - Daniel Vein

Status: Closed
Priority: Normal
Assignee: Community Ticket
Category: Affected Versions: 4.1.2

Description

I probably have something misconfigured but suricata seems to drop traffic on alert on inline.

fast.log

drop.log

09/26/2019-20:54:36.968372: IN= OUT= SRC=192.168.1.177 DST=151.101.148.204 LEN=254 TOS=0x00 TTL=64 ID=633 PROTO=TCP SPT=59446 DPT=80 SEQ=851603426 ACK=2847554061 WINDOW=229 ACK PSH RES=0x00 URGP=0
09/26/2019-20:54:36.990844: IN= OUT= SRC=192.168.1.177 DST=151.101.148.204 LEN=260 TOS=0x00 TTL=64 ID=25877 PROTO=TCP SPT=59448 DPT=80 SEQ=1538132105 ACK=905718895 WINDOW=229 ACK PSH RES=0x00 URGP=0
09/26/2019-20:55:07.022267: IN= OUT= SRC=192.168.1.177 DST=151.101.148.204 LEN=254 TOS=0x00 TTL=64 ID=58507 PROTO=TCP SPT=59450 DPT=80 SEQ=2942922343 ACK=886521798 WINDOW=229 ACK PSH RES=0x00 URGP=0
09/26/2019-20:55:07.076369: IN= OUT= SRC=192.168.1.177 DST=151.101.148.204 LEN=260 TOS=0x00 TTL=64 ID=9673 PROTO=TCP SPT=59452 DPT=80 SEQ=3067195188 ACK=693107189 WINDOW=229 ACK PSH RES=0x00 URGP=0
09/26/2019-20:55:37.076534: IN= OUT= SRC=192.168.1.177 DST=151.101.148.204 LEN=262 TOS=0x00 TTL=64 ID=9673 PROTO=TCP SPT=59454 DPT=80 SEQ=4164996812 ACK=343723356 WINDOW=229 ACK PSH RES=0x00 URGP=0
09/26/2019-20:56:07.114465: IN= OUT= SRC=192.168.1.177 DST=151.101.148.204 LEN=262 TOS=0x00 TTL=64 ID=58023 PROTO=TCP SPT=59458 DPT=80 SEQ=661661500 ACK=699528539 WINDOW=229 ACK PSH RES=0x00 URGP=0

History

#1 - 09/28/2019 11:33 PM - Daniel Vein
user@debian:/var/run/suricata$ sudo suricata c /etc/suricata/suricata.yaml -q 0 -q 1 --user suri --group suri -vvv
28/9/2019 - 18:27:32: Notice: This is Suricata version 4.1.2 RELEASE
28/9/2019 -- 18:27:32 - <Info> - CPUs/cores online: 8
28/9/2019 -- 18:27:32 - <Config> - 'default' server has 'request-body-minimal-inspect-size' set to 33812 and 'request-body-inspect-window' set to 4206 after randomization.
28/9/2019 -- 18:27:32 - <Config> - SMB stream depth: 0
28/9/2019 -- 18:27:32 - <Info> - allocated 262144 bytes of memory for the host hash... 4096 buckets of size 64
28/9/2019 -- 18:27:32 - <Config> - allocated 262144 bytes of memory for the host hash... 4096 buckets of size 64
28/9/2019 -- 18:27:32 - <Config> - preallocated 1000 hosts of size 136
28/9/2019 -- 18:27:32 - <Config> - preallocated 3670016 bytes of memory for the defrag hash... 65536 buckets of size 56
28/9/2019 -- 18:27:32 - <Config> - stream "prealloc-sessions": 2048 (per thread)
28/9/2019 -- 18:27:32 - <Config> - stream.reassembly "depth": 1048576
28/9/2019 -- 18:27:32 - <Info> - dropped the caps for main thread
28/9/2019 -- 18:27:32 - <Config> - enabling 'eve-log' module 'http'
28/9/2019 -- 18:27:32 - <Config> - enabling 'eve-log' module 'dns'
28/9/2019 -- 18:27:32 - <Config> - enabling 'eve-log' module 'files'
28/9/2019 -- 18:27:32 - <Config> - enabling 'eve-log' module 'smtp'
28/9/2019 -- 18:27:32 - <Config> - enabling 'eve-log' module 'nfs'
28/9/2019 -- 18:27:32 - <Config> - enabling 'eve-log' module 'smb'
28/9/2019 -- 18:27:32 - <Config> - enabling 'eve-log' module 'ikev2'
28/9/2019 -- 18:27:32 - <Config> - enabling 'eve-log' module 'krb5'
28/9/2019 -- 18:27:32 - <Config> - enabling 'eve-log' module 'dhcp'
28/9/2019 -- 18:27:32 - <Config> - enabling 'eve-log' module 'sshd'
28/9/2019 -- 18:27:32 - <Config> - enabling 'eve-log' module 'stats'
28/9/2019 -- 18:27:32 - <Config> - enabling 'eve-log' module 'flow'
28/9/2019 -- 18:27:32 - <Config> - Delayed detect disabled
28/9/2019 -- 18:27:37 - <Info> - 1 rule files processed. 23665 rules successfully loaded, 0 rules failed
28/9/2019 -- 18:27:37 - <Info> - Threshold config parsed: 0 rule(s) found
28/9/2019 -- 18:27:38 - <Perf> - using shared mmap cxt' for udp-packet
28/9/2019 -- 18:27:38 - <Perf> - using shared mmap cxt' for other-ip
28/9/2019 -- 18:27:38 - <Perf> - using shared mmap cxt' for http_request_line
28/9/2019 -- 18:27:38 - <Perf> - using shared mmap cxt' for http_accept
28/9/2019 -- 18:27:38 - <Perf> - using shared mmap cxt' for http_accept_enc
28/9/2019 -- 18:27:38 - <Perf> - using shared mmap cxt' for http_accept
28/9/2019 -- 18:27:38 - <Perf> - using shared mmap cxt' for http_start
28/9/2019 -- 18:27:38 - <Perf> - using shared mmap cxt' for http_start
06/12/2020
#2 - 10/01/2019 10:33 PM - Andreas Herz
- Assignee set to Community Ticket
- Target version set to Support

How do you run suricata and how does your config look like?
Also did you change the "alert" keyword to "drop" for those rules?

#3 - 10/02/2019 09:09 PM - Daniel Vein
- File suricata.yaml.txt added

I used drop.conf to change rules and tested that drop rules do drop and show [drop] on fast.log but alert rules show [*] in fast.log but show drops in drop.log. I did not change alert to drop with those rules.

Attached is my suricata.yaml. The only things I changed were the rules directory to work with suricata-update instead of oinkmaster, where the pid file is located, and where the unix socket is located so I could drop privileges. FYI I tested without dropping privileges and still getting packets dropped when they should be alerting

My systemd file:

[Unit]
Description=Suricata IDS/IDP daemon
After=network.target network-online.target
Requires=network-online.target
Documentation=man:suricata(8) man:suricatasc(8)
Documentation=https://suricata-ids.org/docs/

[Service]
Type=forking
Environment=LD_PRELOAD=/usr/lib/x86_64-linux-gnu/libtcmalloc_minimal.so.4
#PIDFile=/var/run/suricata.pid
ExecStart=/usr/bin/suricata -D -c /etc/suricata/suricata.yaml -q 0 -q 1 --user suri --group suri -vvv
ExecReload=/usr/bin/suricatasc /var/run/suricata/custom.socket -c reload-rules ; /bin/kill -HUP $MAINPID
ExecStop=/usr/bin/suricatasc /var/run/suricata/custom.socket -c shutdown
ExecStopPost=/usr/bin/rm /var/run/suricata/suricata.pid
Restart=on-failure
ProtectSystem=full
ProtectHome=true

[Install]
WantedBy=multi-user.target

#4 - 10/04/2019 10:38 PM - Daniel Vein
I was able to figure it out I had rule set to drop but it never triggered an alert.

alert http any any -> any any (msg:="SURICATA TRAFFIC-ID: Debian APT-GET"; content="debian.org"; http_host; content="Debian APT"; http_user_agent; flow:to_server,established; flowbits.set,traffic/id/debian-apt; flowbits.set,traffic/label/software-update; noalert; sid:300000000;)

In the rule it says "noalert" does that mean it won't show alert? Or is because this rule and ET rule 2013504 overlap, and that only triggered the ET rule?

Thanks in advanced and you can close this ticket!

#5 - 10/07/2019 08:41 PM - Andreas Herz
- Status changed from New to Closed

Yes that's expected behaviour. The 'noalert' means it won't show an alert and it also won't drop.