Suricata - Bug #2861

Suricata rule sid:2224005 SURICATA IKEv2 weak cryptographic parameters (Diffie-Hellman) not works

03/04/2019 11:49 AM - Michal Vymazal

Status: Closed
Priority: Normal
Assignee: Pierre Chifflier
Category:
Target version: TBD
Affected Versions:
Effort: Difficulty: Label:

Description
This rule
alert ikev2 any any -> any any (msg:"SURICATA IKEv2 weak cryptographic parameters (Diffie-Hellman)"; flow:to_client; app-layer-event:iikev2.weak_crypto_prf; classtype:protocol-command-decode; sid:2224005; rev:1;)

Doesn't detect weak modp 1024 Diffie-Hellmann parameter

pcap file attached

1. suricata --build-info
   
   This is Suricata version 4.1.0-dev (rev 8709a20d)

Related issues:
Copied to Bug #2865: Suricata rule sid:2224005 SURICATA IKEv2 weak cryptographic parameters (Diffie-Hellman) not works (4.1.x) added

History

#1 - 03/04/2019 02:40 PM - Victor Julien
- Assignee set to Pierre Chifflier

Pierre, could you check this one as well? Thanks!

#2 - 03/04/2019 04:22 PM - Pierre Chifflier

Thanks for the pcap!

A first look at the code shows that internally the weak DH parameters are correctly detected (https://github.com/OISF/suricata/blob/master-4.1.x/rust/src/ikev2/ikev2.rs#L310-L311).

However, I confirm that while the transaction is created and the event is set, no alert is raised. I'm investigating further.

Note: I have found some problems with names in 'rules/ipsec-events.rules', so I'll also fix this.

#3 - 03/04/2019 09:29 PM - Pierre Chifflier
- Status changed from New to Resolved

After investigating, I found 3 causes for the problem:

1. the default rules in rules/ipsec-events.rules are testing flow:to_client. This is not a bug, but is intentional: the server reply contains the accepted proposals, this has greater severity, for ex, than a client proposing weak DH (that can be ignored by the server). If you want to detect weak proposals, you need to either add a rule, or modify the existing one

2. the default rules contained wrong event names. This is fixed in proposed the PR (commit https://github.com/OISF/suricata/pull/3702/commits/d991b2d1ae479d4b56deb460e7611ae676c08324a)

3. a logic bug in the transaction handling for IKEv2 caused the events raised in the first message to be ignored. This is fixed in the proposed PR (commit https://github.com/OISF/suricata/pull/3702/commits/4362525cebeef90ccbb834e306b5e79f48d9f3c0f36)

Marking bug as resolved.

#4 - 03/06/2019 06:12 PM - Victor Julien
- Copied to Bug #2865: Suricata rule sid:2224005 SURICATA IKEv2 weak cryptographic parameters (Diffie-Hellman) not works (4.1.x) added

06/13/2020 1/2
#5 - 06/15/2019 09:54 PM - Andreas Herz
- Target version set to TBD

#6 - 07/29/2019 08:43 PM - Andreas Herz
- Status changed from Resolved to Closed

commits merged

Files
IKEv2_SA_INIT_2-8-weak.pcap 308 Bytes 03/04/2019 Michal Vymazal