Suricata - Bug #149

FN on suricata with i(cmp)type:9

05/06/2010 01:50 AM - rmkml rmkml

Status:	Closed	**Start date:**	05/06/2010
Priority:	Normal	**Due date:**	
Assignee:	Victor Julien	**% Done:**	100%
Category:			
Target version:	0.9.1		

Description

Hi,
I have a FN with this (old) signature and joigned pcap:
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP IRDP router advertisement"; itype:9; reference:arachnids,173; reference:bugtraq,578; reference:cve,1999-0875; classtype:misc-activity; sid:363; rev:7;)
Tested on suricata v0.8.2 and yesterday git.
Regards
Rmkml

History

#1 - 05/06/2010 02:27 AM - Victor Julien

- Status changed from New to Assigned

- Assignee set to Victor Julien

- Target version set to 0.9.0

Issue confirmed, looking into it.

#2 - 05/06/2010 02:44 AM - Victor Julien

- Status changed from Assigned to Feedback

It seems to me it's not a FN after all. The signature uses $HOME_NET as destination, and the packet has 255.255.255.255 as dst address. This would not be a part of $HOME_NET, right? Or should it be as 255.255.255.255 is a broadcast address?

#3 - 05/06/2010 03:47 AM - rmkml rmkml

Thx you again Victor for your very good jobs and support!
My description pb is wrong, This signature not firing with another signature.
Please test with theses two signatures on pcap:
alert icmp any any -> any any (msg:"ICMP IRDP router advertisement"; itype:9; classtype:misc-activity; sid:363; rev:7;)
alert ip 200.31.33.70 31337 -> any any (msg:"test1"; content:"|05|"; sid:90003123; rev:1;)
with theses two signatures, no alert firing. If you comment/disable second sig: first sig firing.
Regards
Rmkml

#4 - 05/06/2010 08:19 AM - Victor Julien

- Target version changed from 0.9.0 to 0.9.1

I've been unable to reproduce this issue. Sigs + pcap work fine here. Will continue to investigate the issue.

#5 - 05/10/2010 12:58 PM - Will Metcalf

I have verified this bug on the test rig. The behavior seems to be the same across all operating systems and compiler optimization levels. With both rules enabled we don't get an alert. If we disable the second rule the first rule fires.

alert icmp any any -> any any (msg:"ICMP IRDP router advertisement"; itype:9; classtype:misc-activity; sid:363; rev:7;)
alert ip 200.31.33.70 31337 -> any any (msg:"test1"; content:"|05|"; sid:90003123; rev:1;)

#6 - 05/10/2010 01:28 PM - Victor Julien

I wonder why I can't reproduce the issue. Can you describe the exact steps Will?

#7 - 05/12/2010 10:24 AM - Pablo Rincon

Yesterday I looked at the bug briefly and seems that we are loosing somehow the sgh (with both sigs enabled).

```
531     det_ctx->sgh = SigMatchSignaturesGetSgh(th_v, de_ctx, det_ctx, p);
(gdb)
534     if (det_ctx->sgh == NULL) {
(gdb)
535         SCLogDebug("no sgh for this packet, nothing to match against");
```

With just the first sig it get's an sgh. Any idea of recent changes related to sgh grouping? The "pass" action implementation didn't change that part of the code at all. Also, commenting the ordering functions call doesn't fix the issue.

#8 - 05/14/2010 03:26 PM - Victor Julien

- Status changed from Feedback to Closed

- % Done changed from 0 to 100

Fixed in current git master.

Files

exemple_icmp_irdp_routeradvertisement.pcap	100 Bytes	05/06/2010	rmkml rmkml