Suricata - Bug #3109

dcerpc engine not generating alerts

08/09/2019 11:02 PM - Travis Green

Status: Feedback
Priority: Normal
Assignee: OISF Dev
Category: 
Target version: Soon
Affected Versions: 
Difficulty: 
Effort: 
Label: 

Description

Rules using dce* keywords do not generate an alert despite matching packet contents. For example, given these two rules:

```alert tcp any any -> $HOME_NET any (msg:"TGI LATERAL DCERPC ATSVC v1.0 Bind UUID 1ff70682-0a51-30e8-076d-740be8cee98b", flow:established; dce_iface:1ff70682-0a51-30e8-076d-740be8cee98b, any_frag; reference:url,401trg.com/an-introduction-to-smb-for-network-security-analysts/; classtype:attempted-admin; sid:2610115; rev:1; metadata:notworking;)
```

```alert tcp any any -> $HOME_NET any (msg:"TGI LATERAL DCERPC ATSVC v1.0 Bind UUID"; flow:established; content:"|82 06 f7 1f 51 0a e8 30 07 6d 74 0b e8 ce e9 8b|"; reference:url,401trg.com/an-introduction-to-smb-for-network-security-analysts/; classtype:attempted-admin; sid:2610113; rev:1;)
```

and this packet: [https://imgur.com/a/necQQvy](https://imgur.com/a/necQQvy)

An alert is only generated for the rule that does not use dce_iface. Pcap attached for repro.

History

### #1 - 08/09/2019 11:04 PM - Travis Green

Eric Leblond had this deeper analysis to offer:

```regit 4:39 PM
ok so here we are:
Diff
diff --git a/rust/src/smb/detect.rs b/rust/src/smb/detect.rs
index c3b890eef..1ab8f3f4d 100644
--- a/rust/src/smb/detect.rs
+++ b/rust/src/smb/detect.rs
@@ -182,13 +182,13 @@ pub extern "C" fn rs_smb_tx_get_dce_iface(state: &mut SMBState,
let is_dcerpc_request = match tx.type_data {
    Some(SMBTransactionTypeData::DCERPC(ref x)) => { x.req_cmd == 1 },
    _ => { false },
};
```

```if !is_dcerpc_request {
    return 0;
-}
+}
```

```let ifaces = match state.dcerpc_ifaces {
    Some(ref x) => x,
    _ => {
```

```let uuid = unsafe{std::slice::from_raw_parts(uuid_ptr, uuid_len as usize)};
-    SCLogDebug!("looking for UUID {:?}", uuid);
+    SCLogNotice!("looking for UUID {:?}", uuid);
```

```for i in ifaces {
    SCLogDebug!("stored UUID {:?} acked {} ack_result {}", i, i.acked, i.ack_result);
+    SCLogNotice!("stored UUID {:?} acked {} ack_result {}", i, i.acked, i.ack_result);
```

06/13/2020
First code is working only on request
second if is forcing check on fact the iface is acked and the ack_result is 0
First point: this contrdict a previous commit https://github.com/OISF/suricata/commit/c4b56ca28917eb460ea9eb2
23b9bc98fbb9e1d8
so we have a bug
second point: I don't know enough the protocol but for me, if we specify a match on iface and we have iface we should have a match any way
@tgreen with this patch I got 2 alerts
on signature that was failing
tgreen profile image
regit 4:55 PM
tgreen profile image
Second point: I don't know enough the protocol but for me, if we specify a match on iface and we have iface we should have a match any way
Syslog message from 30/09/2019 22:17:25
This is Suricata version 5.0.0-dev

#2 - 08/10/2019 08:35 AM - Eric Leblond
Side note: the pcap needs stream.midstream to true to get properly analysed but this does not alert correctly after that.

#3 - 08/12/2019 07:26 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#4 - 09/17/2019 05:12 PM - Victor Julien
Can you create (a) SV test case(s)?

#5 - 09/26/2019 07:44 AM - Victor Julien
Can you test against: Suricata 4.1.5 (no rust), 4.1.5 (with rust) and git master?

#6 - 09/26/2019 07:45 AM - Victor Julien
- Status changed from New to Feedback
- Assignee changed from OISF Dev to Travis Green
- Target version changed from TBD to Soon

#7 - 10/14/2019 04:05 PM - Travis Green
Submitted PR for suricata-verify test https://github.com/OISF/suricata-verify/pull/139

#8 - 10/21/2019 07:49 PM - Travis Green

```plaintext
---
$ cat /dev/null > ./fast.log && sudo /opt/suricata-git.latest/src/suricata -c
/etc/suricata/suricata.testsuite4.yaml -1 -S ~/rules/lateral-rules/lateral.rules -k none -r ./merged.pcap &&
cat ./fast.log & & wc ./fast.log
This is Suricata version 5.0.0-dev (412a11ba 2019-10-12) running in USER mode
<snip>
56 1331 14696 ./fast.log
---

$ cat /dev/null > ./fast.log && sudo /opt/suricata-git.debug/src/suricata -c
/etc/suricata/suricata.testsuite4.yaml -1 -S ~/rules/lateral-rules/lateral.rules -k none -r ./merged.pcap &&
cat ./fast.log & & wc ./fast.log
This is Suricata version 5.0.0-dev (494617bb3 2019-09-12) running in USER mode
<snip>
42 974 10832 ./fast.log
---

$ cat /dev/null > ./fast.log && sudo /opt/suricata-git.debug/src/suricata -c
/etc/suricata/suricata.testsuite4.yaml -1 -S ~/rules/lateral-rules/lateral.rules -k none -r ./merged.pcap &&
cat ./fast.log & & wc ./fast.log
21/10/2019 -- 12:36:49 - <Notice> - This is Suricata version 4.1.5 RELEASE
<snip>
```

06/13/2020
$ cat /dev/null > ./fast.log && sudo /opt/suricata-4.1.5.norust/src/suricata -c /etc/suricata/suricata.testsuri4.yaml -l . -S ~/rules/lateral-rules/lateral.rules -k none -r ./merged.pcap && cat ./fast.log && wc ./fast.log

21/10/2019 -- 12:36:54 -- <Notice> -- This is Suricata version 4.1.5 RELEASE
46 1076 11936 ./fast.log

details @ https://gist.github.com/travisbgreen/e3b34e848efbe2fe0dc37183786ce9be

#9 - 02/25/2020 02:11 PM - Victor Julien
- Assignee changed from Travis Green to OISF Dev

Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>20171220_smb_at_schedule.pcap</td>
<td>3.53 KB</td>
<td>08/09/2019</td>
<td>Travis Green</td>
</tr>
</tbody>
</table>