### Suricata - Bug #3109

dcerpc engine not generating alerts

<table>
<thead>
<tr>
<th>Status:</th>
<th>Feedback</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>OISF Dev</td>
</tr>
<tr>
<td>Category:</td>
<td>TBD</td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

**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", 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,
    ifaces = match state.dcerpc_ifaces {
        Some(ref x) => x,
        _ => {
@@ -197,12 +197,13 @@ pub extern "C" fn rs_smb_tx_get_dce_iface(state: &mut SMBState,
            uuid = unsafe{std::slice::from_raw_parts(uuid_ptr, uuid_len as usize)};
        }
    }
```

An alert is only generated for the rule that does not use dce_iface. pcap attached for repro.
#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 07:45 AM - Victor Julien

Can you test against: Suricata 4.1.5 (no rust), 4.1.5 (with rust) and git master?

#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 - 09/17/2019 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 70

#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

---


29956] 21/10/2019 12:36:49 - <Notice> - This is Suricata version 4.1.5 RELEASE


21/10/2019 -- 12:36:49 - <Notice> - This is Suricata version 4.1.5 RELEASE

---
$ cat /dev/null > ./fast.log &
$ sudo /opt/suricata-4.1.5.norust/src/suricata -c
/etc/suricata/suricata.testuri4.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

I think this works as intended: bind followed by a request. IIRC this was done for Snort compatibility.

I agree it would be nicer to be able to just match on the bind, but I don't want to break existing rules either.

Perhaps we need a new set of keywords where compatibility doesn't have to be taken into account.

Files

20171220_smb_at_schedule.pcap 3.53 KB 08/09/2019 Travis Green