Suricata - Feature #4398

support regex match and flowvars as keywords value

03/15/2021 10:27 AM - jim cookie

Status: New
Priority: Normal
Assignee:
Category:
Target version: TBD
Effort: medium
Difficulty: medium

Description

if we want to detect java jndi injection such as fastjson rce:
tcp payload content:
ldap://192.168.204.1:888 or rmi://192.168.204.1:888
flow rules just only detect the first steps of jndi injection:
alert tcp any any -> any any
(msg:"TCP_LDAP_Injection";pcre:"/(ldap://(\[(S]{2,256}):([d]{2,5})\)/;flow:ldap,flow:ldap_url,flow:ldap_port";sid:10001;rev:1;
we can found flowvars ldap、ldap_url and ldap_port in eve.json:

```json
{
  "timestamp": "2021-01-12T14:10:04.520436+0800",
  "flow_id": 60042522718452,
  "pcap_cnt": 3,
  "event_type": "alert",
  "src_ip": "192.168.204.130",
  "src_port": 20,
  "dest_ip": "192.168.204.128",
  "dest_port": 80,
  "proto": "TCP",
  "metadata": {
    "flowvars": [
      {"ldap": "ldap://192.168.204.1:888/"},
      {"ldap_url": "192.168.204.1"},
      {"ldap_port": 888}]
  },
  "alert": {"action": "allowed", "gid": 1, "signature_id": 10001, "rev": 1,
    "signature": "TCP_LDAP_Injection", "category": "", "severity": 3,
    "flow": {"pkts_toserver": 1, "bytes_toserver": 84,"bytes_toclient": 0,"start": "2021-01-12T14:10:04.520436+0800",
      "payload": "R0VUIC9sZGFwOi8vMTkyLjE2OC4yMDQuMTo4ODgv", "payload_printable": "GET /ldap://192.168.204.1:888/"},
    "stream": 0}
```

but, we can't detect the hackers ladp server : 192.168.204.1 connection .

if we suricata support use regex match and flowvars as keywords value . we can creat rules like this:

alert tcp any any -> any any
(msg:"TCP_LDAP_Injection_steps1";pcre:"/(ldap://(\[(S]{2,256}):([d]{2,5})\)/;flow:ldap,flow:ldap_url,flow:ldap_port";noalert;sid:10001;rev:1;)
alert tcp any any -> $ldap_url $ldap_port (msg:"TCP_LDAP_Injection_success";sid:10002;rev:1;)
maby also with xbits work great more.

have any other ways to detect jndi injection ?
thanks you !

History

#1 - 03/15/2021 11:48 AM - Victor Julien
- Description updated
- Assignee deleted (Shivani Bhardwaj)
- Target version changed from 6.0.2 to TBD

Files

TCP_LDAP_success.pcap 761 Bytes 03/15/2021 jim cookie