Sign in

splunk / security_content Public

Notifications | Fork 359 | Star 1.3k

Code | Issues 21 | Pull requests 13 | Discussions | Actions | Projects | Wiki | S

security_content / detections / endpoint / petitpotam_suspicious_kerberos_tgt_request.yml

61 lines (61 loc) · 3.36 KB

Code | Blame | Raw

```yaml
name: PetitPotam Suspicious Kerberos TGT Request
id: e3ef244e-0a67-11ec-abf2-acde48001122
version: 4
date: '2024-09-30'
author: Michael Haag, Mauricio Velazco, Splunk
status: production
type: TTP
description: The following analytic detects a suspicious Kerberos Ticket Granting Ticket (TGT) requ
data_source:
- Windows Event Log Security 4768
search: '`wineventlog_security` EventCode=4768 src!="::1" TargetUserName=*$ CertThumbprint!="" | st
how_to_implement: The following analytic requires Event Code 4768. Ensure that it is logging no Dom
known_false_positives: False positives are possible if the environment is using certificates for au
references:
- https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4768
- https://isc.sans.edu/forums/diary/Active+Directory+Certificate+Services+ADCS+PKI+domain+admin+vul
drilldown_searches:
- name: View the detection results for - "$dest$"
  search: '%original_detection_search% | search  dest = "$dest$"'
  earliest_offset: $info_min_time$
  latest_offset: $info_max_time$
- name: View risk events for the last 7 days for - "$dest$"
  search: '| from datamodel Risk.All_Risk | search normalized_risk_object IN ("$dest$") starthoursa
  earliest_offset: $info_min_time$
  latest_offset: $info_max_time$
tags:
  analytic_story:
  - PetitPotam NTLM Relay on Active Directory Certificate Services
  - Active Directory Kerberos Attacks
  asset_type: Endpoint
  confidence: 70
  cve:
  - CVE-2021-36942
  impact: 80
  message: A Kerberos TGT was requested in a non-standard manner against $dest$, potentially relate
  mitre_attack_id:
  - T1003
  observable:
  - name: dest
    type: Hostname
    role:
    - Victim
  product:
  - Splunk Enterprise
  - Splunk Enterprise Security
  - Splunk Cloud
  required_fields:
  - _time
  - dest
  - Account_Name
  - Client_Address
  - action
  - Message
  risk_score: 56
  security_domain: endpoint
tests:
- name: True Positive Test
  attack_data:
  - data: https://media.githubusercontent.com/media/splunk/attack_data/master/datasets/attack_techn
    source: XmlWinEventLog:Security
    sourcetype: XmlWinEventLog
```