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_network_share_access_request.yml

70 lines (67 loc) · 2.64 KB

Code Blame Raw

```yaml
name: PetitPotam Network Share Access Request
id: 95b8061a-0a67-11ec-85ec-acde48001122
version: 1
date: '2021-08-31'
author: Michael Haag, Mauricio Velazco, Splunk
type: TTP
datamodel: []
description: 'The following analytic utilizes Windows Event Code 5145, "A network
  share object was checked to see whether client can be granted desired access". During
  our research into PetitPotam, CVE-2021-36942, we identified the ocurrence of this
  event on the target host with specific values. \

  To enable 5145 events via Group Policy - Computer Configuration->Polices->Windows
  Settings->Security Settings->Advanced Audit Policy Configuration. Expand this node,
  go to Object Access (Audit Polices->Object Access), then select the Setting Audit
  Detailed File Share Audit \

  It is possible this is not enabled by default and may need to be reviewed and enabled.
  \

  During triage, review parallel security events to identify further suspicious activity.'
search: '`wineventlog_security` Account_Name="ANONYMOUS LOGON" EventCode=5145 Relative_Target_Name=
  | stats count min(_time) as firstTime max(_time) as lastTime by dest, Security_ID,
  Share_Name, Source_Address, Accesses, Message | `security_content_ctime(firstTime)`
  | `security_content_ctime(lastTime)` | `petitpotam_network_share_access_request_filter`'
how_to_implement: Windows Event Code 5145 is required to utilize this analytic and
```

```yaml
  it may not be enabled in most environments.
known_false_positives: False positives have been limited when the Anonymous Logon
  is used for Account Name.
references:
- https://attack.mitre.org/techniques/T1187/
- https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=5145
- https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5145
tags:
  analytic_story:
  - PetitPotam NTLM Relay on Active Directory Certificate Services
  dataset:
  - https://media.githubusercontent.com/media/splunk/attack_data/master/datasets/attack_techniques/
  kill_chain_phases:
  - Exploitation
  - Lateral Movement
  mitre_attack_id:
  - T1187
  product:
  - Splunk Enterprise
  - Splunk Enterprise Security
  - Splunk Cloud
  required_fields:
  - _time
  - dest
  - Security_ID
  - Share_Name
  - Source_Address
  - Accesses
  - Message
  security_domain: endpoint
  impact: 80
  confidence: 70
  risk_score: 56
  context:
  - Source:Endpoint
  - Stage:Credential Access
  message: A remote host is enumerating a $dest$ to identify permissions. This is
    a precursor event to CVE-2021-36942, PetitPotam.
  observable:
  - name: dest
    type: Hostname
    role:
    - Victim
  automated_detection_testing: passed
```