detection-rules / rules / _deprecated / privilege_escalation_krbrelayup_suspicious_logon.toml

Samirbous and DefSecSentinel [Deprecated Rule] Potential Privi... 8d34416 · 2 years ago History

```
1   [metadata]
2   creation_date = "2022/04/26"
3   deprecation_date = "2022/08/01"
4   maturity = "deprecated"
5   updated_date = "2022/08/01"
6
7   [rule]
8   author = ["Elastic"]
9   description = """
10  Identifies a suspicious local successful logon event where the Logon Package is Kerbero
11  localhost, and the target user SID is the built-in local Administrator account. This ma
12  a Kerberos relay attack variant that can be used to elevate privilege locally from a do
13  System privileges.
14  """
15  from = "now-9m"
16  index = ["winlogbeat-*", "logs-system.*"]
17  language = "eql"
18  license = "Elastic License v2"
19  name = "Potential Privilege Escalation via Local Kerberos Relay over LDAP"
```

detection-rules / rules / _deprecated / privilege_escalation_krbrelayup_suspicious_logon.toml Top

Code Blame 75 lines (62 loc) · 2.31 KB Raw

```
24  ]
25  risk_score = 73
26  rule_id = "3605a013-6f0c-4f7d-88a5-326f5be262ec"
27  severity = "high"
28  tags = ["Elastic", "Host", "Windows", "Threat Detection", "Privilege Escalation", "Cred
29  type = "eql"
30
31  query = '''
32  authentication where
33
34   /* event 4624 need to be logged */
35   event.action == "logged-in" and event.outcome == "success" and
36
37   /* authenticate locally via relayed kerberos ticket */
38   winlog.event_data.AuthenticationPackageName : "Kerberos" and winlog.logon.type == "Net
39   source.ip == "127.0.0.1" and source.port > 0 and
40
41   /* Impersonate Administrator user via S4U2Self service ticket */
42   winlog.event_data.TargetUserSid : "S-1-5-21-*-500"
43  '''
44
45
46  [[rule.threat]]
47  framework = "MITRE ATT&CK"
48  [[rule.threat.technique]]
49  id = "T1548"
50  name = "Abuse Elevation Control Mechanism"
51  reference = "https://attack.mitre.org/techniques/T1548/"
52  [[rule.threat.technique.subtechnique]]
53  id = "T1548.002"
54  name = "Bypass User Account Control"
55  reference = "https://attack.mitre.org/techniques/T1548/002/"
```

command_and_control_sql_ser...
command_and_control_ssh_se...
command_and_control_ssh_se...
command_and_control_tor_act...
credential_access_potential_lin...
credential_access_tcpdump_act...
defense_evasion_attempt_to_d...
defense_evasion_base64_enco...
defense_evasion_code_injectio...
defense_evasion_execution_via...
defense_evasion_hex_encoding...
defense_evasion_ld_preload_en...
defense_evasion_mshta_makin...
defense_evasion_potential_pro...
defense_evasion_whitespace_p...
discovery_file_dir_discovery.toml
discovery_process_discovery_vi...
discovery_query_registry_via_r...
discovery_whoami_commman...
execution_apt_binary.toml
execution_awk_binary_shell.toml
execution_busybox_binary.toml
execution_c89_c99_binary.toml

```
56
57
58
59      [rule.threat.tactic]
60      id = "TA0004"
61      name = "Privilege Escalation"
62      reference = "https://attack.mitre.org/tactics/TA0004/"
63      [[rule.threat]]
64      framework = "MITRE ATT&CK"
65      [[rule.threat.technique]]
66      id = "T1558"
67      name = "Steal or Forge Kerberos Tickets"
68      reference = "https://attack.mitre.org/techniques/T1558/"
69
70
71      [rule.threat.tactic]
72      id = "TA0006"
73      name = "Credential Access"
74      reference = "https://attack.mitre.org/tactics/TA0006/"
```