



elastic / **detection-rules** Public

Notifications

Fork 498

Star 2k

<> Code

Issues 145

Pull requests 21

Actions

Security

Insights

detection-rules / rules / \_deprecated / privilege\_escalation\_krbrelayup\_suspicious\_logon.toml

75 lines (62 loc) · 2.31 KB

Code

Blame

Raw

```
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 Kerberos, the remot
11 localhost, and the target user SID is the built-in local Administrator account. This may indicate a
12 a Kerberos relay attack variant that can be used to elevate privilege locally from a domain joined
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"
20 references = [
21     "https://github.com/Dec0ne/KrbRelayUp",
22     "https://googleprojectzero.blogspot.com/2021/10/using-kerberos-for-authentication-relay.html",
23     "https://github.com/cube0x0/KrbRelay",
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", "Credential Access"]
29     type = "eq1"
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 == "Network" and
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/"
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/"
```