

Product

Solutions

Resources

Open Source

Enterprise

Pricing

Sign in

Sign up

elastic

/ detection-rules

Public

Notifications

Fork

498

Star

2k

<> Code

Issues

144

Pull requests

28

Actions

Security

Insights

Files

4312d8c

Go to file

> .github

> detection_rules

> docs

> kibana

> kql

> rta

> rules

> _deprecated

> apm

> cross-platform

> integrations

> linux

> macos

credential_access_access_to_br...

credential_access_credentials_k...

credential_access_dumping_ha...

credential_access_dumping_ke...

credential_access_kerberosdu...

credential_access_keychain_pw...

credential_access_mitm_localh...

credential_access_potential_ma...

credential_access_prompt_for_p...

credential_access_systemkey_d...

defense_evasion_apple_softup...

defense_evasion_attempt_del...

defense_evasion_attempt_to_d...

defense_evasion_install_root_c...

defense_evasion_modify_envir...

defense_evasion_privacy_contr...

defense_evasion_privilege_esca...

defense_evasion_safari_config...

defense_evasion_sandboxed_of...

defense_evasion_tcc_bypass_m...

defense_evasion_unload_endp...

discovery_users_domain_built_i...

execution_defense_evasion_ele...

detection-rules / rules / macos / persistence_enable_root_account.toml

terrancedejesus and Mikaayenson

[FR] Add Endpoint, APM and...

4312d8c · 2 years ago

History

Code

Blame

51 lines (43 loc) · 1.42 KB

Raw

1

[metadata]

2

creation_date = "2020/01/04"

3

integration = ["endpoint"]

4

maturity = "production"

5

min_stack_comments = "New fields added: required_fields, related_integrations, setup"

6

min_stack_version = "8.3.0"

7

updated_date = "2022/12/14"

8

9

[rule]

10

author = ["Elastic"]

11

description = ""

12

Identifies attempts to enable the root account using the dsenableroot command. This com

13

for persistence, as the root account is disabled by default.

14

""

15

from = "now-9m"

16

index = ["auditbeat-*", "logs-endpoint.events.*"]

17

language = "kuery"

18

license = "Elastic License v2"

19

name = "Attempt to Enable the Root Account"

20

references = ["https://ss64.com/osx/dsenableroot.html"]

21

risk_score = 47

22

rule_id = "cc2fd2d0-ba3a-4939-b87f-2901764ed036"

23

severity = "medium"

24

tags = ["Elastic", "Host", "macOS", "Threat Detection", "Persistence"]

25

timestamp_override = "event.ingested"

26

type = "query"

27

28

query = '''

29

event.category:process and event.type:(start or process_started) and

30

process.name:dsenableroot and not process.args:"-d"

31

'''

32

33

34

[[rule.threat]]

35

framework = "MITRE ATT&CK"

36

[[rule.threat.technique]]

37

id = "T1078"

38

name = "Valid Accounts"

39

reference = "https://attack.mitre.org/techniques/T1078/"

40

[[rule.threat.technique.subtechnique]]

41

id = "T1078.003"

42

name = "Local Accounts"

43

reference = "https://attack.mitre.org/techniques/T1078/003/"

44

45

46

47

[rule.threat.tactic]

48

id = "TA0003"

49

name = "Persistence"

50

reference = "https://attack.mitre.org/tactics/TA0003/"

Page 1 of 2

- 📄 execution_initial_access_suspici...
- 📄 execution_installer_package_sp...
- 📄 execution_script_via_automato...
- 📄 execution_scripting_osascript_e...
- 📄 execution_shell_execution_via_...
- 📄 initial access suspicious mac ...