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

```toml
[metadata]
creation_date = "2020/01/04"
integration = ["endpoint"]
maturity = "production"
min_stack_comments = "New fields added: required_fields, related_integrations, setup"
min_stack_version = "8.3.0"
updated_date = "2022/12/14"

[rule]
author = ["Elastic"]
description = """
Identifies attempts to enable the root account using the dsenableroot command. This com
for persistence, as the root account is disabled by default.
"""
from = "now-9m"
index = ["auditbeat-*", "logs-endpoint.events.*"]
language = "kuery"
license = "Elastic License v2"
name = "Attempt to Enable the Root Account"
references = ["https://ss64.com/osx/dsenableroot.html"]
risk_score = 47
rule_id = "cc2fd2d0-ba3a-4939-b87f-2901764ed036"
severity = "medium"
tags = ["Elastic", "Host", "macOS", "Threat Detection", "Persistence"]
timestamp_override = "event.ingested"
type = "query"

query = '''
event.category:process and event.type:(start or process_started) and
 process.name:dsenableroot and not process.args:"-d"
'''


[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1078"
name = "Valid Accounts"
reference = "https://attack.mitre.org/techniques/T1078/"
[[rule.threat.technique.subtechnique]]
id = "T1078.003"
name = "Local Accounts"
reference = "https://attack.mitre.org/techniques/T1078/003/"



[rule.threat.tactic]
id = "TA0003"
name = "Persistence"
reference = "https://attack.mitre.org/tactics/TA0003/"
```

- execution_initial_access_suspici…
- execution_installer_package_sp…
- execution_script_via_automato…
- execution_scripting_osascript_e…
- execution_shell_execution_via_…
- initial_access_suspicious_mac_…