Modification of Environment Variable via Launchctl | Elastic Security [7.17]

Archived: 2026-04-05 17:20:05 UTC

Modification of Environment Variable via Launchctl

edit

Identifies modifications to an environment variable using the built-in launchctl command. Adversaries may execute their own malicious payloads by hijacking certain environment variables to load arbitrary libraries or bypass certain restrictions.

Rule type: query

Rule indices:

- auditbeat-*
- logs-endpoint.events.*

Severity: medium

Risk score: 47

Runs every: 5m

Searches indices from: now-9m (Date Math format, see also `Additional look-back time`)

Maximum alerts per execution: 100

References:

- https://github.com/rapid7/metasploit-framework/blob/master//modules/post/osx/escalate/tccbypass.rb

Tags:

- Elastic
- Host
- macOS
- Threat Detection
- Defense Evasion

Version: 5

Rule authors:

- Elastic

Rule license: Elastic License v2

```
event.category:process and event.type:start and
  process.name:launchctl and
  process.args:(setenv and not (JAVA*_HOME or
                                RUNTIME_JAVA_HOME or
                                DBUS_LAUNCHD_SESSION_BUS_SOCKET or
                                ANT_HOME or
                                LG_WEBOS_TV_SDK_HOME or
                                WEBOS_CLI_TV or
                                EDEN_ENV)
                ) and
  not process.parent.executable:("/Applications/NoMachine.app/Contents/Frameworks/bin/nxserver.bin" (
                                 "/usr/local/bin/kr" or
                                 "/Applications/NoMachine.app/Contents/Frameworks/bin/nxserver.bin" (
                                 "/Applications/IntelliJ IDEA CE.app/Contents/jbr/Contents/Home/lib/
  not process.args : "*.vmoptions"
```

Framework: MITRE ATT&CK™

- Tactic:
  - Name: Defense Evasion
  - ID: TA0005
  - Reference URL: https://attack.mitre.org/tactics/TA0005/
- Technique:
  - Name: Hijack Execution Flow
  - ID: T1574
  - Reference URL: https://attack.mitre.org/techniques/T1574/
- Sub-technique:
  - Name: Path Interception by PATH Environment Variable
  - ID: T1574.007
  - Reference URL: https://attack.mitre.org/techniques/T1574/007/
