Binary Executed from Shared Memory Directory | Elastic Security [7.17]

Binary Executed from Shared Memory Directory

edit

Identifies the execution of a binary by root in Linux shared memory directories: (/dev/shm/, /run/shm/, /var/run/, /var/lock/). This activity is to be considered highly abnormal and should be investigated. Threat actors have placed executables used for persistence on high-uptime servers in these directories as system backdoors.

Rule type: eql

Rule indices:

- logs-endpoint.events.*

Severity: high

Risk score: 73

Runs every: 5m

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

Maximum alerts per execution: 100

References:

- https://linuxsecurity.com/features/fileless-malware-on-linux
- https://twitter.com/GossiTheDog/status/1522964028284411907

Tags:

- Elastic
- Host
- Linux
- Threat Detection
- Execution
- BPFDoor

Version: 1

Rule authors:

- Elastic

Rule license: Elastic License v2

```
process where event.type == "start" and
    event.action == "exec" and user.name == "root" and
    process.executable : (
        "/dev/shm/*",
        "/run/shm/*",
        "/var/run/*",
        "/var/lock/*"
    )
```

Framework: MITRE ATT&CK™

- Tactic:
    - Name: Execution
    - ID: TA0002
    - Reference URL: https://attack.mitre.org/tactics/TA0002/
- Technique:
    - Name: Command and Scripting Interpreter
    - ID: T1059
    - Reference URL: https://attack.mitre.org/techniques/T1059/
