Endpoint Resource Saturation and Crash Pattern Detection Across Platforms, Detection Strategy DET0208

Archived: 2026-04-02 10:46:27 UTC

AN0584

Excessive resource exhaustion or service crash induced by processes launched by users or scripts that rapidly consume CPU/memory or attempt malformed service interactions.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Number of service crashes or high-CPU events within a defined time period
ServiceTarget	Specific service name or executable targeted for DoS (e.g., svchost.exe, w3wp.exe)
CPUThresholdPercent	CPU usage percent considered anomalous over duration

AN0585

Malicious script or binary causes repeated kernel panics, OOM kills, or systemd service restarts targeting services like nginx, httpd, sshd.

Log Sources

Mutable Elements

Field	Description
ServiceName	Targeted daemon/service such as sshd, nginx, mysql
RestartThreshold	Number of restarts in short succession to trigger alert
OOMKillCount	Count of OOM kills over a time window

AN0586

Adversary launches high-entropy process or malformed app bundle causing repeated application crashes and system slowdowns.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	macos:unifiedlog	Repeated process crashes logged by CrashReporter or system instability logs in com.apple.console
Host Status (DC0018)	macos:unifiedlog	Spike in CPU or memory use from non-user-initiated processes

Mutable Elements

Field	Description
CrashCountThreshold	Number of app crashes within monitoring window
PayloadEntropyThreshold	Used for high-entropy binaries often observed in DoS malware samples

AN0587

Instance enters degraded/unhealthy state due to abnormal process load or memory exhaustion, often caused by automation or script-based attacks.

Log Sources

Mutable Elements

Field	Description
InstanceType	Burstable vs compute-optimized instances impact DoS effect
FailureThreshold	How many consecutive StatusCheckFailed events to consider critical

AN0588

Container orchestrator logs show crashlooping pods, repeated resource exhaustion, or malicious binaries with infinite loops consuming systemd/cgroup limits.

Log Sources

Mutable Elements

Field	Description
RestartCountThreshold	Number of container restarts within a time window

Field	Description
ContainerImageEntropy	Payload entropy of container image as an anomaly factor

---