Detection Strategy for Endpoint DoS via Application or System Exploitation, Detection Strategy DET0304

Archived: 2026-04-02 12:12:12 UTC

AN0850

Exploitation of system or application vulnerability (e.g., CVE-based exploit) followed by service crash, restart, or repeated failure within a short time frame, impacting application/system availability.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time window between repeated service crashes or restarts (e.g., 5 crashes within 1 hour)
TargetApplication	Critical applications to monitor based on environment (e.g., web server, database, VPN)

AN0851

User or remote input triggers application crash or segmentation fault (e.g., SIGSEGV) with service recovery attempts, observed via audit logs and systemd journaling.

Log Sources

Mutable Elements

Field	Description
CrashPattern	Specific binary fault signature or stack trace identifiers unique to the application context
ExploitSourceIP	Suspect source IPs for correlation across requests and service failure timing

AN0852

Application crash or repeated restart cycle triggered by malformed input or exploit file, observed via unified logs and process crash monitoring.

Log Sources

Mutable Elements

Field	Description
CrashSignature	Binary crash hash or affected dylib for distinguishing malicious faults from benign ones
InputVector	File, IPC, or network-based input that may be triggering exploitation (e.g., PDF file, POST request)

AN0853

Cloud workload exploitation leads to repeated container, service, or VM termination/restart, typically associated with CVE-based crash triggers or fuzzed payloads.

Log Sources

Mutable Elements

Field	Description
CrashThreshold	Number of repeated crashes or terminations observed before triggering alert
ServiceID	Cloud service name, workload, or container ID to scope alerting

---