Process Access, Data Component DC0035

Archived: 2026-04-05 14:43:12 UTC

Refers to an event where one process attempts to open another process, typically to inspect or manipulate its memory, access handles, or modify execution flow. Monitoring these access attempts can provide valuable insight into both benign and malicious behaviors, such as debugging, inter-process communication (IPC), or process injection.

Data Collection Measures:

- Endpoint Detection and Response (EDR) Tools:
  - EDR solutions that provide telemetry on inter-process access and memory manipulation.
- Sysmon (Windows):
  - Event ID 10: Captures process access attempts, including:
    - Source process (initiator)
    - Target process (victim)
    - Access rights requested
    - Process ID correlation
- Windows Event Logs:
  - Event ID 4656 (Audit Handle to an Object): Logs access attempts to system objects.
  - Event ID 4690 (Attempted Process Modification): Can help identify unauthorized process changes.
- Linux/macOS Monitoring:
  - AuditD: Monitors process access through syscall tracing (e.g., `ptrace`, `open`, `read`, `write`).
  - eBPF/XDP: Used for low-level monitoring of kernel process access.
  - OSQuery: Query process access behavior via structured SQL-like logging.
- Procmon (Process Monitor) and Debugging Tools:
  - Windows Procmon: Captures real-time process interactions.
  - Linux strace / ptrace: Useful for tracking process behavior at the system call level.

Source: https://attack.mitre.org/datacomponents/DC0035