Detection of Denial of Service, Detection Strategy DET0723

Archived: 2026-04-05 17:30:13 UTC

AN1856

Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g., extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g., monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).
Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.
Monitor for application logging, messaging, and/or other artifacts that may result from Denial of Service (DoS) attacks which degrade or block the availability of services to users. In addition to network level detections, endpoint logging and instrumentation can be useful for detection.
Monitor operational data for indicators of temporary data loss which may indicate a Denial of Service. This will not directly detect the technique’s execution, but instead may provide additional evidence that the technique has been used and may complement other detections.

Log Sources
