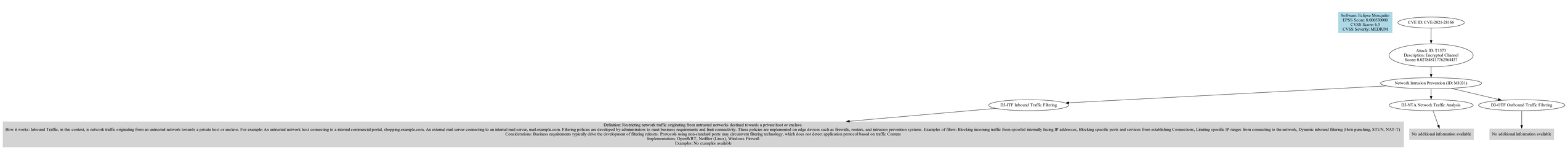
Software: Eclipse Mosquitto
EPSS Score: 0.00030000
CVSS Score: 6.5
CVSS Severity: MEDIUM
CVE ID: CVE-2021-28166
Attack ID: T1573
Description: Encrypted Channel
Score: 0.027844117762964437
Network Intrusion Prevention (ID: M1031)
D3-ITF Inbound Traffic Filtering
D3-NTA Network Traffic Analysis
D3-OTF Outbound Traffic Filtering
Definition: Restricting network traffic originating from untrusted networks destined towards a private host or enclave.
How it works: Inbound Traffic, in this context, is network traffic originating from an untrusted network towards a private host or enclave. For example: An untrusted network host connecting to a internal commercial portal, shopping.example.com, An external mail server connecting to an internal mail server, mail.example.com. Filtering policies are developed by administrators to meet business requirements and limit connectivity. These policies are implemented on edge devices such as firewalls, routers, and intrusion prevention systems. Examples of filters: Blocking incoming traffic from spoofed internally facing IP addresses, Blocking specific ports and services from establishing Connections, Limiting specific IP ranges from connecting to the network, Dynamic inbound filtering (Hole punching, STUN, NAT-T)
Considerations: Business requirements typically drive the development of filtering rulesets. Protocols using non-standard ports may circumvent filtering technology, which does not detect application protocol based on traffic Content
Implementations: OpenWRT, Netfilter (Linux), Windows Firewall
Examples: No examples available
No additional information available
No additional information available