Threat Description: The SNORT rule is designed to detect MySQL connection attempts by monitoring traffic directed at TCP port 3306, the default port used by MySQL servers. This rule triggers an alert whenever a TCP connection is established to a MySQL service, which can be indicative of legitimate database access, but also potentially unauthorized scanning or enumeration attempts. Attackers may probe this port to identify open databases or weak configurations as part of a larger reconnaissance or exploitation campaign.

Indicators of Compromise (IoCs)

Destination Port: 3306 (default MySQL port)

Protocol: TCP

Direction: Incoming to MySQL server

Source: Any IP / Any Port

Detection Mechanism:

Matches any TCP traffic going to port 3306

msg:"MySQL connection detected": Generates an alert message

Possible Attribution & Use Cases:

Database administrators performing remote connections

Attackers scanning for exposed MySQL services

Malware attempting to exfiltrate or access data via MySQL

Penetration testers assessing database exposure

Recommended Actions:

Monitor and Investigate: Confirm whether the connection is authorized. Investigate unknown source IPs connecting to port 3306.

Restrict Access: Limit MySQL access using firewalls, VPNs, and network segmentation.

Log and Alert: Continuously log MySQL access attempts and generate alerts for unusual patterns.

Secure MySQL Instances: Ensure authentication is strong and that MySQL is not exposed to the public internet unless necessary.

Author & Attribution:

Rule Author: Community

Rule Source:

SID: 1000011

Revision: 1