Threat Category: Reconnaissance, RPC

Threat Description: The rule is designed to detect attempts to list RPC services on TCP port 32771. This activity is characteristic of reconnaissance scans that attackers use to identify potential targets and vulnerabilities within a network. The rule specifically looks for the RPC portmap listing request, which if successful, provides information about available RPC services and their corresponding ports. This information can be leveraged by attackers to target specific services for exploitation.

Indicators of Compromise (IoCs)

Destination Port: 32771

RPC Program Number: 100000 (0x186A0)

RPC Version: 2

RPC Procedure: 4

Detection Mechanism:

Checks for the presence of the RPC program number 100000 (0x186A0) at offset 16 with a depth of 4 bytes.

Verifies the RPC version is 2 (0x00000002).

Looks for RPC procedure 4 (PMAP_DUMP).

The rule uses the flow:to_server,established; keyword to ensure that the detection occurs on established connections going to the server.

Possible Attribution & Use Cases:

Attackers use portmap listing to discover vulnerable RPC services.

The detection can be used to identify potential reconnaissance activity on a network.

Recommended Actions:

Monitor and Investigate: Analyze the source IP address to determine the origin of the scan. Investigate any suspicious activity originating from the source.

Restrict Access: Implement firewall rules to restrict access to port 32771 from untrusted networks.

Author & Attribution:

Rule Author: community

Rule Source:

SID: 599

Revision: 17