

Threat Category: Attempted Denial of Service (DoS), Malicious Use of ICMP

Threat Description: The rule is designed to detect the use of the Tribe Flood Network client command "LE" via ICMP. This rule specifically looks for ICMP traffic from an external network to an internal network. The detection mechanism focuses on identifying specific values within the ICMP header and payload. It checks for an ICMP ID of 51201, an ICMP sequence number of 0, and an ICMP type of 0 (Echo Reply). Additionally, it uses a PCRE (Perl Compatible Regular Expression) to match a pattern of `"/^[0-9]{1,5}\x00/"` in the ICMP payload.

Indicators of Compromise (IoCs):

ICMP Type: 0 (Echo Reply)

ICMP ID: 51201

ICMP Sequence: 0

PCRE Pattern: `"/^[0-9]{1,5}\x00/"` (in ICMP payload)

Detection Mechanism: This rule identifies potential TFN "LE" command usage using the following conditions:

The network protocol must be ICMP.

The traffic direction must be from `$EXTERNAL_NET` to `$HOME_NET`.

The ICMP type must be 0 (Echo Reply).

The ICMP ID must be 51201.

The ICMP sequence number must be 0.

The ICMP payload must match the PCRE pattern `"/^{1,5}\x00/"`.

Possible Attribution & Use Cases:

This rule is useful for monitoring network traffic for malicious ICMP activity and potential DoS

attacks.

Recommended Actions:

Monitor and Investigate: If this rule is triggered, investigate the source of the ICMP traffic to determine the intent and potential impact of the TFN "LE" command.

Rate Limiting: Implement rate limiting on ICMP traffic to mitigate potential DoS attacks.

Firewall Configuration: Configure firewalls to restrict or block suspicious ICMP traffic.

Intrusion Detection: Utilize intrusion detection systems to identify and alert on malicious ICMP activity.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Reference: CVE-2000-0138

Rule SID: 251

Rule Revision: 11