Threat Category: Protocol Anomaly, Buffer Overflow, NNTP Exploit

Threat Description: The SNORT rule is designed to detect a buffer overflow attempt in the Network News Transfer Protocol (NNTP). This rule focuses on traffic from an external network to an internal network on TCP port 119. The detection mechanism involves checking the NNTP return code and ensuring that if the return code is "200", the subsequent data exceeds a certain length. Specifically, it checks for the content "200", uses isdataat to ensure there are at least 256 bytes following, and employs a PCRE to match a string starting with "200" followed by 256 or more non-newline characters.

Indicators of Compromise (IoCs):

TCP Port: 119 (NNTP)

Content: "200"

PCRE Pattern: ?/^200\s[^\n]{256}/ims?

Detection Mechanism:

The network protocol must be TCP.

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

The source port must be 119.

The TCP connection must be established (established).

The content must contain "200".

There must be at least 256 bytes of data following "200" (isdataat).

The PCRE pattern must match, indicating a "200" response followed by an excessively long string.

Possible Attribution & Use Cases:

The detection can be used to identify attempts to exploit buffer overflow vulnerabilities in NNTP servers.

This rule is useful for monitoring network traffic for potentially malicious NNTP commands.

Recommended Actions:

Monitor and Investigate: If this rule is triggered, investigate the targeted NNTP server for potential compromise.

Patching: Ensure that NNTP servers are patched against known buffer overflow vulnerabilities.

Intrusion Prevention: Utilize intrusion prevention systems to block NNTP exploit attempts.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 1792

Rule Revision: 16

Reference: Bugtraq-4900, CVE-2002-0909