Threat Category: Protocol Anomaly, Buffer Overflow, POP3 Exploit

Threat Description: This rule is designed to detect a buffer overflow attempt in the Post Office Protocol version 3 (POP3) AUTH command. This rule focuses on traffic from an external network to an internal network on TCP port 110. The detection mechanism involves checking for the "AUTH" command and ensuring that the subsequent data exceeds a certain length. Specifically, it checks for the content "AUTH" (case-insensitive), uses isdataat to ensure there are at least 50 bytes following, and employs a PCRE to match a string starting with "AUTH" followed by 50 or more non-newline characters.

Indicators of Compromise (IoCs):

TCP Port: 110 (POP3)

Content: "AUTH" (case-insensitive)

PCRE Pattern: ?/^AUTH\s[^\n]{50}/ims?

Detection Mechanism:

The network protocol must be TCP.

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

The destination port must be 110.

The TCP connection must be established (established).

The content must contain "AUTH" (case-insensitive).

There must be at least 50 bytes of data following "AUTH" (isdataat).

The PCRE pattern must match, indicating an "AUTH" command followed by an excessively long string.

Possible Attribution & Use Cases:

The detection can be used to identify attempts to exploit buffer overflow vulnerabilities in POP3

servers.

This rule is useful for monitoring network traffic for potentially malicious POP3 commands.

Recommended Actions:

Monitor and Investigate: If this rule is triggered, investigate the targeted POP3 server for potential compromise.

Patching: Ensure that POP3 servers are patched against known buffer overflow vulnerabilities.

Intrusion Prevention: Utilize intrusion prevention systems to block POP3 exploit attempts.

Disable POP3: If possible, disable the POP3 service and use more secure alternatives such as IMAP.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 1936

Rule Revision: 14

Service: pop3

Reference: Bugtraq-830, CVE-1999-0822, Nessus-10184S