Threat Category: Protocol Anomaly, Buffer Overflow, FTP Exploit

Threat Description: The rule is designed to detect SITE CHMOD overflow attempts in the File Transfer Protocol (FTP). This rule focuses on traffic from an external network to an internal network on TCP port 21. The detection mechanism involves checking for the "SITE CHMOD" command sequence and ensuring that the subsequent data exceeds a certain length. Specifically, it checks for the content "SITE" (case-insensitive), the content "CHMOD" (case-insensitive) with a distance of 0, uses isdataat to ensure there are at least 200 bytes following, and employs a PCRE to match a string starting with "SITE CHMOD" followed by 200 or more non-newline characters.

Indicators of Compromise (IoCs):

TCP Port: 21 (FTP)

Content 1: "SITE" (case-insensitive)

Content 2: "CHMOD" (case-insensitive, distance 0)

PCRE Pattern: ?/^SITE\s+CHMOD\s[^\n]{200}/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 21.

The TCP connection must be established (established).

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

The content must contain "CHMOD" (case-insensitive) immediately following "SITE".

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

The PCRE pattern must match, indicating a "SITE CHMOD" 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 FTP servers via the SITE CHMOD command.

Recommended Actions:

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

Patching: Ensure that FTP servers are patched against known buffer overflow vulnerabilities related to the SITE CHMOD command.

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

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 2340

Rule Revision: 15

Service: ftp

Reference: Bugtraq-10181, Bugtraq-9483, Bugtraq-9675, CVE-1999-0838, Nessus-12037