Threat Category: Operating System Exploit, Attempted Administrator Privilege Gain, Solaris Specific Exploit

Threat Description: The SNORT rule is designed to detect attempts to exploit a SPARC overflow vulnerability in Solaris systems. This rule specifically looks for TCP traffic from an external network to an internal network on port 53 (DNS). The detection mechanism focuses on identifying specific byte sequences within the TCP packet payload. The rule checks for the presence of the following hexadecimal byte sequences: "|90 1A C0 0F 90 02| |08 92 02| |0F D0 23 BF F8|" using fast_pattern and nocase matching. These specific byte patterns are indicative of an attempt to exploit this Solaris vulnerability.

Indicators of Compromise (IoCs):

TCP Port: 53 (DNS)

Hexadecimal Byte Sequences: "|90 1A C0 0F 90 02| |08 92 02| |0F D0 23 BF F8|"

Detection Mechanism:

The network protocol must be TCP.

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

The destination port must be 53 (DNS).

The TCP connection must be established (established).

The payload must contain the hexadecimal byte sequences "|90 1A C0 0F 90 02| |08 92 02| |0F D0 23 BF F8|".

The rule uses fast_pattern for efficient matching and nocase to ensure case-insensitive matching of the byte sequences.

Possible Attribution & Use Cases: The detection can be used to identify attempts to gain unauthorized access or execute arbitrary code on Solaris systems.

Recommended Actions:

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

Patching: Ensure that all Solaris systems are patched with the latest security updates to mitigate the vulnerability.

Network Security: Implement network security measures, such as firewalls and intrusion prevention systems, to block or detect exploit attempts.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 267

Rule Revision: 13

Service: DNS