Threat Category: Protocol Anomaly, Buffer Overflow, RPC Exploit

Threat Description: The SNORT rule is designed to detect a yppasswd username overflow attempt via UDP. This rule focuses on traffic from an external network to an internal network. The detection mechanism involves checking for specific byte sequences within the UDP packet payload at specific offsets and depths, along with byte jumps and tests. Specifically, it checks for "|00 01 86 A9|" at a depth of 4 and offset of 12, "|00 00 00 01|" within 4 bytes with a distance of 4, a series of byte jumps, a byte test, and "|00 00 00 00|" at a depth of 4 and offset of 4. These patterns and operations are indicative of an attempt to exploit a buffer overflow in the yppasswd service.

Indicators of Compromise (IoCs):

Content Pattern 1: "|00 01 86 A9|" (depth 4, offset 12)

Content Pattern 2: "|00 00 00 01|" (within 4, distance 4)

Byte Jumps and Tests

Content Pattern 3: "|00 00 00 00|" (depth 4, offset 4)

Detection Mechanism:

The network protocol must be UDP.

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

The payload must contain the specified content patterns at the specified depths and offsets.

The rule includes a series of byte_jump operations to navigate through the packet structure.

The rule uses a byte_test to check if a value is greater than 64.

Possible Attribution & Use Cases:

The detection can be used to identify attempts to exploit buffer overflow vulnerabilities in the yppasswd service, potentially gaining unauthorized access.

This rule is useful for monitoring network traffic for potentially malicious RPC activity.

Recommended Actions:

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

Patching: Ensure that systems running the yppasswd service are patched against known buffer overflow vulnerabilities.

Restrict Access: Implement firewall rules to restrict access to the yppasswd service from untrusted networks.

Intrusion Detection: Utilize intrusion detection systems to identify and alert on yppasswd exploit attempts.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 2025

Rule Revision: 17

Metadata: policy max-detect-ips drop

Reference: Bugtraq-2763, CVE-2001-0779, Nessus-10684