WHITEHATS

- What's New
- About Whitehats
- Infosec Library
- Contact Us
- Terms Of Use
- Privacy Policy

- **Intrusion Detection**
  - . arachNIDS Center
  - . Mailing List *
  - . Submit Signatures
  - . Forum: General NIDS
  - . Forum: arachNIDS
  - . Forum: Signatures
  - . Forum: Snort IDS
  - . IDS Tools
- **Penetration Testing**
  - . Forum: Penetration
  - . Forum: Nessus
  - . Assessment Tools
- **Network Defense**
  - . Forum: DDOS Attacks
  - . Forum: Internet Law
  - . Forum: Incidents
  - . Defense Tools

Search arachNIDS

Search Tools

Search Forums

arachNIDS - The Intrusion Event Database

browse by grouping, classification, target affected

Event | Protocol | Research | Signatures

IDS13/RPC_PORTMAP-REQUEST-MOUNTD

Summary

This event indicates that a query was sent to the portmap daemon, requesting port information for the rpc.mountd service. This query usually precedes attempts to access mountd, access NFS, or to attack the rpc.mountd service with protocol or buffer overflow conditions.

How Specific

This event is specific to a vulnerability, but may have been caused by any of several possible exploits. Packet payload is not considered in the signatures used to detect this attack.

Trusting The Source IP Address

Since this event was caused by a UDP packet, the source IP address could be easily forged. It has been noted that the intruder is likely to expect or desire a response to their packets, so it may be likely that the source IP address is not spoofed.

Platform(s):	unix
Category:	rpc
Classification:	Information Gathering Attempt
CVE	CAN-1999-0632
Bugtraq	nomatch
advICE	2001733

Protocol details... *(ip header, tcp/udp/icmp header, payload data)*
Research details... *(packet captures, background, credits)*
IDS Signatures... *(dynamically generated signatures for free and commercial IDS)*