



Home | Security Forums | Free Tools | arachNIDS

[Wednesday, July 18]

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

arachNIDS - The Intrusion Event Database

browse by [grouping](#), [classification](#), [target affected](#)

[Event](#)
[Protocol](#)
[Research](#)
[Signatures](#)

IDS15/RPC_PORTMAP-REQUEST-STATUS

Summary

This event indicates that a query was sent to the portmap daemon, requesting port information for the status service. This query usually precedes attempts to access status.

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.

[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*)

Platform(s): unix
Category: rpc
Classification: Information Gathering Attempt

CVE [CAN-1999-0632](#)
Bugtraq nomatch
advICE [2001733](#)

Search arachNIDS

Search Tools

Search Forums

Copyright © 2001 Whitehats, Inc. All rights reserved.

© 2001 [Whitehats, Inc.](#) All rights reserved. [Contact Us](#)