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

IDS481/MISC_SOCKS-OVERFLOW-X86LINUX

Summary

This event indicates that an attempt had been made to compromise a linux server by exploiting a overflow a buffer vulnerability in the socks proxy software.

How Specific

This event is specific to a particular exploit and is detected based on a particular string of characters found in the packet payload. Signatures for this event are very specific.

Platform(s):	linux
Category:	misc
Classification:	System Integrity Attempt
CVE	nomatch
Bugtraq	154
advICE	nomatch

Trusting The Source IP Address

The packet that caused this event is normally a part of an established TCP session, indicating that the source IP address has not been spoofed. If you are using a firewall that supports stateful inspection, and are not vulnerable to sequence number prediction attacks, then you can be fairly certain that the source IP address of the event is accurate. 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)*