WHITEHATS

Home | **Security Forums** | **Free Tools** | **arachNIDS** *[Friday, July 20]*

- **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

IDS8/TELNET_TELNET-DAEMON-ACTIVE

Platform(s):	unix windows device
Category:	telnet
Classification:	Suspicious
CVE	CAN-1999-0619
Bugtraq	nomatch
advICE	nomatch

Summary

This event indicates that a successful telnet connection has been established from outside the local network. Telnet is a very insecure protocol and should be replaced with SSH immediately.

How Specific

This event is specific to a vulnerability, but may have been caused by any of several possible exploits. Signatures used to detect this event are specific and consider the packet payload.

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)*